

CIS Microsoft Azure Storage Services Benchmark

v1.0.0 - 11-15-2024

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (CISLegal@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	7
Important Usage Information	7
Key Stakeholders	7
Apply the Correct Version of a Benchmark	8
Exceptions	8
Remediation	9
Summary	9
Target Technology Details	10
Intended Audience.....	10
Consensus Guidance	11
Typographical Conventions.....	12
Recommendation Definitions.....	13
Title.....	13
Assessment Status.....	13
Automated	13
Manual.....	13
Profile	13
Description.....	13
Rationale Statement	13
Impact Statement.....	14
Audit Procedure.....	14
Remediation Procedure.....	14
Default Value.....	14
References	14
CIS Critical Security Controls® (CIS Controls®).....	14
Additional Information.....	14
Profile Definitions	15
Acknowledgements	16
Recommendations	17
1 Introduction.....	17
1.1 CIS Microsoft Azure Foundations Benchmarks	17
1.2 CIS Microsoft Azure Service Category Benchmarks	19
1.3 Multiple Methods of Audit and Remediation.....	20
2 Common Reference Recommendations	22

2.1 Secrets and Keys	23
2.1.1 Shared Access Signatures	24
2.1.1.1 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)	25
2.1.1.2 Ensure that shared access signature (SAS) tokens expire within an hour (Manual) ...	27
2.1.1.3 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)	29
2.1.2 Encryption Key Management	31
2.1.2.1 Microsoft Managed Keys	32
2.1.2.1.1 Ensure Critical Data is Encrypted with Microsoft Managed Keys (MMK) (Manual) ..	33
2.1.2.2 Customer Managed Keys	35
2.1.2.2.1 Ensure Critical Data is Encrypted with Customer Managed Keys (CMK) (Manual) ..	36
2.1.2.3 Customer Provided Keys	38
2.2 Networking	39
2.2.1 Virtual Networks (VNETs)	40
2.2.1.1 Ensure public network access is Disabled (Automated)	41
2.2.1.2 Ensure Network Access Rules are set to Deny-by-default (Automated)	43
2.2.2 Private Endpoints	45
2.2.2.1 Ensure Private Endpoints are used to access {service} (Automated)	46
2.2.3 Private Link	48
2.3 Identity and Access Management	49
2.4 Logging	50
3 Archive Storage (Reference)	51
Resources for Archive Storage	51
4 Azure Managed Lustre	52
Resources for Azure Managed Lustre	52
4.1 Ensure 'Key encryption key' is set to a customer-managed key for Azure Managed Lustre file systems (Automated)	53
5 Azure Backup	57
Resources for Azure Backup	57
5.1 Backup Vaults	58
Resources for Backup vaults	58
5.1.1 Ensure soft delete on Backup vaults is Enabled (Automated)	59
5.1.2 Ensure immutability for Backup vaults is Enabled (Automated)	62
5.1.3 Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK) (Automated)	65
5.1.4 Ensure 'Use infrastructure encryption for this vault' is enabled on Backup vaults (Automated)	68
5.1.5 Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults (Automated)	72
5.1.6 Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults (Automated)	75
5.2 Recovery Services Vaults	79
Resources for Recovery Services vaults	79
5.2.1 Ensure soft delete on Recovery Services vaults is Enabled (Automated)	80
5.2.2 Ensure immutability for Recovery Services vaults is Enabled (Automated)	83
5.2.3 Ensure backup data in Recovery Services vaults is encrypted using customer-managed keys (CMK) (Automated)	86
5.2.4 Ensure 'Use infrastructure encryption for this vault' is enabled on Recovery Services vaults (Automated)	90
5.2.5 Ensure public network access on Recovery Services vaults is Disabled (Automated) ...	94
5.2.6 Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults (Automated)	97
5.2.7 Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults (Automated)	100

6 Azure Data Lake Storage (Reference)	104
Resources for Azure Data Lake Storage	104
7 Azure Data Share	105
Resources for Azure Data Share	105
8 Azure Files	106
Resources for Azure Files	106
8.1 Ensure soft delete for Azure File Shares is Enabled (Automated)	107
8.2 Ensure root squash for NFS file shares is configured (Automated)	110
8.3 Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares (Automated)	113
8.4 Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares (Automated)	116
9 Azure Storage Actions (Preview)	119
Resources for Azure Storage Actions	119
10 Azure NetApp Files	120
Resources for Azure NetApp Files	120
10.1 Ensure 'Encryption key source' is set to 'Customer Managed Key' for Azure NetApp Files accounts (Automated)	121
11 Azure Blob Storage	124
Resources for Azure Blob Storage	124
11.1 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)	125
11.2 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	127
11.3 Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled (Automated)	129
11.4 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)	131
11.5 Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts (Automated)	134
11.6 Ensure locked immutability policies are used for containers storing business-critical blob data (Automated)	138
12 Azure Data Box	141
Resources for Azure Data Box	141
12.1 Ensure double encryption is used for Azure Data Box in high-security environments (Manual)	142
13 Azure Disk Storage (Reference)	144
Resources for Azure Disk Storage	144
14 Azure Confidential Ledger	145
Resources for Azure Confidential Ledger	145
15 Azure Elastic SAN	146
Resources for Azure Elastic SAN	146
15.1 Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN (Automated)	147
15.2 Ensure customer-managed keys (CMK) are used to encrypt data at rest on Azure Elastic SAN volume groups (Automated)	150
16 Queue Storage	154
Resources for Queue Storage	154
16.1 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)	155
16.2 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	157

16.3 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual).....	159
17 Storage Accounts	162
Resources for Storage Accounts	162
17.1 Secrets and Keys	163
17.1.1 Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)	164
17.1.2 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual).....	167
17.1.3 Ensure that Storage Account Access Keys are Periodically Regenerated (Manual) ..	169
17.1.4 Ensure that shared access signature (SAS) tokens expire within an hour (Manual) ..	172
17.1.5 Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled' (Automated)	174
17.1.6 Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) (Manual)	178
17.2 Networking	181
17.2.1 Ensure Private Endpoints are used to access Storage Accounts (Automated)	182
17.2.2 Ensure that 'Public Network Access' is 'Disabled' for storage accounts (Automated)	187
17.2.3 Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated)	190
17.3 Identity and Access Management	193
17.4 Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)	194
17.5 Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled' (Automated).....	196
17.6 Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated).....	199
17.7 Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)....	202
17.8 Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated)	205
17.9 Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated)	208
17.10 Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated)	211
17.11 Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2' (Automated)	214
17.12 Ensure 'Cross Tenant Replication' is not enabled (Automated)	217
17.13 Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled' (Automated).....	219
17.14 Ensure Azure Resource Manager Delete locks are applied to Azure Storage Accounts (Manual)	222
17.15 Ensure Azure Resource Manager ReadOnly locks are considered for Azure Storage Accounts (Manual)	225
17.16 Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts (Automated)	229
18 Storage Explorer.....	232
Resources for Storage Explorer	232
18.1 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	233
18.2 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual).....	235
18.3 Ensure Storage Explorer is using the latest version (Manual)	238
19 Azure Container Storage.....	240
Resources for Azure Container Storage	240
Appendix: Summary Table	241
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	248

<i>Appendix: CIS Controls v7 IG 2 Mapped Recommendations</i>	<i>250</i>
<i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations</i>	<i>253</i>
<i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i>	<i>257</i>
<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations</i>	<i>258</i>
<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations</i>	<i>261</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>265</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>269</i>
<i>Appendix: Change History</i>	<i>270</i>

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

This benchmark - CIS Microsoft Azure Storage Services Benchmark - will provide secure configuration recommendations for Azure products that Microsoft has categorized as “Storage” services in the Azure Products Directory (<https://azure.microsoft.com/en-us/products/#storage>).

The specific Microsoft Azure services in scope of this Benchmark include:

- Archive Storage
- Azure Managed Lustre
- Azure Backup
- Azure Data Lake Storage
- Azure Data Share
- Azure Files
- Azure Storage Actions
- Azure NetApp Files
- Azure Blob Storage
- Azure Data Box
- Azure Disk Storage
- Azure Confidential Ledger
- Azure Elastic SAN
- Queue Storage
- Storage Accounts
- Storage Explorer
- Azure Container Storage

For more information on Microsoft Azure product categories and services, please refer to the Microsoft Azure Product Directory here: <https://azure.microsoft.com/en-us/products/>.

To obtain the latest version of this guide, please visit <https://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at BenchmarkInfo@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Azure.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<code><Monospace font in brackets></code>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide security focused best practice hardening of a technology; and
- limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability
- acts as defense in depth measure
- may impact the utility or performance of the technology
- may include additional licensing, cost, or addition of third party software

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor

Krishna Rayavaram
Gareth Boyes

Editor

Rachel Rice
Ian McRee
Steve Johnson

Recommendations

1 Introduction

This introduction section and the subsections herein provide informative articles which instruct on the use of the CIS Foundations and Service Category Benchmarks. No recommendations will be found in this section, just articles of relevant information.

Please carefully review the articles in this introductory section and orient yourself with our structured approach to Benchmarking for Cloud Service Providers (CSPs). This approach differs from other CIS Benchmarks because:

- there are too many different products/services in CSP product directories to practically cover in any one Benchmark,
- architectural and design decisions will affect the scope and relevance of recommendations, and
- there are a variety of methods for interfacing with CSP products and services.

Cloud Benchmarks - A Two-Step Approach to Securing Your Cloud Environments:

- **Step 1:** Start with Foundations Benchmarks. Apply as many recommendations as **practical** for your environment; "100%" 'compliance' is not always possible. Not all Foundations Benchmark recommendations can be applied at the same time, and not all recommendations will be relevant to your environment. Use the recommendation Profile Levels and your understanding of your unique environment architecture to determine which recommendations are in scope.
- **Step 2:** Use the Service Category Benchmarks for service-specific defense-in-depth recommendations. Apply recommendations only for the services **IN USE** in your environment. Use the recommendation Profile Levels, and your understanding of your unique environment architecture to determine which recommendations are in scope.

1.1 CIS Microsoft Azure Foundations Benchmarks

The suggested approach for securing your Microsoft Azure cloud environment is to start with the **latest version** of the CIS Microsoft Azure Foundations Benchmark. Because CSP environments are constantly changing, previous versions of the Foundations Benchmarks should not be used; they are very likely to contain incorrect product names, outdated procedures, deprecated features, and other inaccuracies. The CIS Foundations Benchmark provides prescriptive guidance for configuring a subset of Microsoft Azure Services with an emphasis on foundational, testable, and architecture agnostic settings for services.

The Microsoft Azure Foundation Benchmark is what you should start with when beginning to secure your Azure environment. It is also the foundation for which all other Azure Service Category Benchmarks are built on so that as you grow your cloud presence and usage of the services offered you have the necessary guidance to securely configure your environment as it fits with your company's policy.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS Microsoft Azure Benchmarks, please register on CIS WorkBench at <https://workbench.cisecurity.org> and join the CIS Microsoft Azure Benchmarks Community.

1.2 CIS Microsoft Azure Service Category Benchmarks

After configuring your environment with the CIS Microsoft Azure Foundations Benchmark, we suggest pursuing defense-in-depth and service-specific recommendations for your Azure Services by reviewing the Service Category Benchmarks. The Service Category Benchmarks are being produced with the vision that recommendations for all security-relevant products/services offered by a CSP should have a 'home,' but the Foundations Benchmarks should retain the most crucial recommendations and not be made vast, intimidating, and impractical.

The Service Category Benchmark recommendations should be applied **ONLY** for the CSP products and services that are actively **IN USE** in your environment. In each Service Category Benchmark, you may find that your environment uses none, or only a couple services from a list of many. Please review the services employed in your environment carefully to accurately scope the recommendations you apply. Failure to apply only the recommendations you need may introduce vulnerabilities, technical debt, and unnecessary expenses.

Using the Microsoft Azure Product Directory (<https://azure.microsoft.com/en-us/products/>) as a source of categorical grouping of these services, our vision is to produce a full set of CIS Microsoft Azure Service Category Benchmarks to cover all security-relevant services. A list of planned and published Service Category Benchmarks for the Azure Community can be found on the community dashboard here: <https://workbench.cisecurity.org/communities/72>.

Your help is needed to bring this vision to life! Please consider joining our CIS Microsoft Azure Community to contribute your expertise and knowledge in securing products and services from the Microsoft Azure product family.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS Microsoft Azure Benchmarks, please register on CIS WorkBench at <https://workbench.cisecurity.org> and join the CIS Microsoft Azure Benchmarks community.

1.3 Multiple Methods of Audit and Remediation

Throughout the Benchmark, Audit and Remediation procedures are prescribed using up to five different methods. These multiple methods are presented for the convenience of readers who will be coming from different technical and experiential backgrounds. To perform any given Audit or Remediation, only one method needs to be performed. Not every method is available for every recommendation, and many that are available are not yet written for every recommendation. The methods presented in the Benchmark are formatted and titled as follows:

- **"From Azure Portal"** - This is the administrative GUI accessed at <https://portal.azure.com>.
- **"From Azure CLI"** - See additional detail in the next section.
- **"From PowerShell"** - See additional detail in the next section.
- **"From REST API"** - An Application Programming Interface (API) for HTTP operations on service endpoints.
- **"From Azure Policy"** - Azure Policy is administered from the Microsoft Defender for Cloud blade where Policy Initiatives can be created from "Regulatory Compliance" or by using pre-built Industry & Regulatory Standards.

Setting Up PowerShell and Azure CLI

In order to use the Azure Command Line Interface (CLI) and the Azure PowerShell methods for audit and remediation procedures, the following permissions are required for the account running the procedures:

1. Global Reader
2. Security Reader
3. Subscription Contributor
4. Key Vault Get/List privileges on Keys, Secrets, Certificates, and Certificate Authorities
5. Network allow listing for any source IP address performing the audit activities
6. Permissions to use PowerShell and Azure CLI

These permissions can be directly assigned or assigned via Privileged Identity Management.

The Azure CLI tool can be installed from the following location:

<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli>

For PowerShell, the following cmdlets are required:

1. Azure PowerShell: <https://docs.microsoft.com/en-us/powershell/azure/install-az-ps-msi?view=azps-12.2.0>
2. Microsoft Graph PowerShell: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/get-started?view=graph-powershell-1.0>
3. Azure AD PowerShell for Graph: [***Deprecation Planned**]

4. MS Online PowerShell: [**Deprecation Planned*]

**Deprecation Planned:* Azure AD, Azure AD Preview and MSONline PowerShell modules are planned for deprecation. Microsoft Graph PowerShell is the PowerShell module to use for interacting with Microsoft Entra ID and other Microsoft services. This reference of mapped cmdlets can help where replacement commands are needed: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0>.

Authenticating with Azure CLI

Run the following command from either PowerShell or command prompt:

```
az login --tenant <tenant id> --subscription <subscription ID>
```

Authenticating with PowerShell

Login to the Azure tenant and subscription using the following command:

```
Connect-AzAccount -DeviceCode
```

1. Navigate a browser to <https://microsoft.com/devicelogin>.
2. Enter the code returned from running the **Connect-AzAccount -DeviceCode** command above.
3. When prompted, login with your Azure account credentials or if already authenticated, choose the correct Azure account.
4. If asked **Are you trying to sign into Azure PowerShell?**, click **Continue**.
5. Close the browser or browser tab when completed.

For the remaining PowerShell modules, the log in method is the same for now, though when logging into the **AzureAD** PowerShell module, you may get a warning to use the **MgGraph** PowerShell module instead. To log in to each, run the following commands.

```
Connect-MgGraph  
Connect-AzureAD
```

NOTE: This may store session information within the PowerShell environment and may persist after closing PowerShell. Please take all necessary precautions to shorten the lifespan of this session and protect it from unauthorized access.

2 Common Reference Recommendations

IMPORTANT NOTE: Do not use the recommendations in this section for audit or remediation.

For the services that these recommendations are relevant to, a copy of the reference recommendation with full and accurate audit and remediation procedures will be found in the section dedicated to that service.

This section is intended to provide a generic reference for common recommendation types that are applicable to multiple Products and Services within the CSP environment. Common Reference Recommendations are those that recommend the use of different types of networking or connection methodologies, data or secret protection, or are otherwise generally used throughout the CSP environment and might result in additional duplicate recommendations. These recommendations will be copied to the named Service sections to which they apply and be augmented with audit and remediation procedures that are accurate to the specific Service.

2.1 Secrets and Keys

2.1.1 Shared Access Signatures

2.1.1.1 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signatures (SAS) can be used to grant limited access to Azure Storage resources. When generating a SAS, it is possible to specify the allowed protocols for a request made with the SAS. It is recommended to allow requests over HTTPS only.

Rationale:

If a SAS is passed over HTTP and intercepted, an attacker performing a man-in-the-middle attack can read the SAS. Then, they can use that SAS just as the intended user could have. This can potentially compromise sensitive data or allow for data corruption by the malicious user.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

Remediation:

Default Value:

When generating a SAS, the default selection for **Allowed protocols** is **HTTPS only**.

References:





1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage>

Additional Information:

This recommendation forms the basis for the recommendations with the same title in the following sections:

- **Azure Blob Storage**
- **Queue Storage**
- **Storage Accounts > Secrets and Keys**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

2.1.1.2 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signature (SAS) tokens provide restricted access to Azure Storage resources (such as blobs, files, queues, or tables) for a defined time period with specific permissions. It enables users to interact with the resources without exposing account keys, offering precise control over the permitted actions (e.g., read, write) and the duration of access. To minimize security risks, SAS tokens should be configured with the shortest possible lifespan, ideally lasting no longer than an hour.

Rationale:

A short lifespan for SAS tokens is recommended to minimize the risk of unauthorized access. SAS tokens grant time-limited access to resources, and a longer duration increases the opportunity for misuse if the token is compromised. By setting a shorter lifespan, the potential for security breaches is reduced.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

Remediation:

Default Value:

By default, expiration for shared access signature is set to 8 hours.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature>






Additional Information:

This recommendation forms the basis for the recommendations with the same title in the following sections:

- **Azure Blob Storage**
- **Queue Storage**
- **Storage Accounts > Secrets and Keys**

- Storage Explorer

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 <u>Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 <u>Establish Process for Revoking Access</u> Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

2.1.1.3 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)

Profile Applicability:

- Level 1

Description:

Use stored access policies (SAP) when generating shared access signature (SAS) tokens in Azure to centrally manage permissions, expiration, and revocation settings for resource access. Stored access policies can be applied to blob containers, file shares, queues, and tables.

Rationale:

Stored access policies provide centralized control over SAS token access, allowing administrators to update permissions or revoke access. This approach strengthens security by reducing the risk of unauthorized access to storage resources.

Impact:

There is no cost for creating stored access policies, however there is some administrative overhead involved in managing these policies.

Audit:

Remediation:

Default Value:

By default, stored access policies are not associated with SAS. To use a stored access policy, it must be explicitly created and linked to the SAS at the time of creation.

References:







1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas>
2. <https://learn.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy>

Additional Information:

This recommendation forms the basis for the recommendations with the same title in the following sections:

- Azure Blob Storage
- Queue Storage
- Storage Explorer

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.2 Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<u>14.6 Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

2.1.2 Encryption Key Management

The use of an appropriate Encryption Key Management methodology requires a carefully determined architectural choice that reflects your organization's maturity, technical capabilities, and compliance requirements.

Azure Services generally provide three options for Encryption Key Management:

1. **Microsoft Managed Keys ('MMK')** [Also known as Platform Managed Keys or PMK]: The storage, creation, and maintenance of encryption keys is performed automatically by Microsoft. This option uses the Microsoft key store and automates the control and rotation of keys. Where the security and compliance frameworks implemented by your organization do not specify otherwise, Microsoft Managed Keys is generally preferred, but it should be understood that there is an implied trust that your organization must assume.
2. **Customer Managed Keys ('CMK')**: The creation and maintenance of encryption keys is the responsibility of the customer but stored in a Microsoft provided vault. This option stores keys in Azure Key Vault or Key Vault HSM, but the control and rotation of keys is performed by the customer. Encryption Key management introduces some complexity and technical debt to an environment because the creation and maintenance of keys requires technical capacity for maintaining key infrastructure in addition to scripting for automation. For environments that have specific compliance requirements for the control and rotation of keys, this option may be required.
3. **Customer Provided Keys ('CPK')**: The storage, control, and rotation of encryption keys is the responsibility of the customer. Your organization must have an independent key storage facility, maintain control and perform rotation of keys. This option introduces the most complexity and technical debt and should be implemented only for highly secure environments or systems where compliance requirements specify that key storage must be maintained by your organization.

The use of each of these methods of managing encryption keys requires careful consideration, and the scope of application should be determined prior to implementation.

2.1.2.1 Microsoft Managed Keys

2.1.2.1.1 Ensure Critical Data is Encrypted with Microsoft Managed Keys (MMK) (Manual)

Profile Applicability:

- Level 1

Description:

Microsoft Managed Keys (MMK) [also known as Platform-managed keys (PMK)] provides a very low overhead method of encrypting data at rest and implementing encryption key management. Keys maintained in an MMK implementation are automatically managed by Azure and require no customer interaction.

Rationale:

The encryption of data at rest is a foundational component of data security. Data at rest without encryption is easily compromised through loss or theft. Encrypting data at rest introduces confidentiality to the data by obfuscating the data contents with a cipher algorithm and provides an authentication requirement through the use of cryptographic keys. MMK makes the encryption of data at rest very easy to implement and maintain.




Audit:**Remediation:****Default Value:**

By default, Encryption type is set to Microsoft Managed Keys.

References:

1. <https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-rest>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>
3. <https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

2.1.2.2 Customer Managed Keys

2.1.2.2.1 Ensure Critical Data is Encrypted with Customer Managed Keys (CMK) (Manual)

Profile Applicability:

- Level 2

Description:

Customer Managed Keys introduce additional depth to security by providing a means to manage access control for encryption keys. Where compliance and security frameworks indicate the need, and organizational capacity allows, sensitive data at rest can be encrypted using Customer Managed Keys (CMK) rather than Microsoft Managed keys.

Rationale:

By default in Azure, data at rest tends to be encrypted using Microsoft Managed Keys. If your organization want to control and manage encryption keys for compliance and defense-in-depth, Customer Managed Keys can be established.

While it is possible to automate the assessment of this recommendation, the assessment status for this recommendation remains 'Manual' due to ideally limited scope. The scope of application - which workloads CMK is applied to - should be carefully considered to account for organizational capacity and targeted to workloads with specific need for CMK.

Impact:

If the key expires due to setting the 'activation date' and 'expiration date', the key must be rotated manually.

Using Customer Managed Keys may also incur additional man-hour requirements to create, store, manage, and protect the keys as needed.

Audit:

Remediation:




Default Value:

By default, Encryption type is set to Microsoft Managed Keys.

References:

1. <https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-rest>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

2.1.2.3 Customer Provided Keys

2.2 Networking

2.2.1 Virtual Networks (VNets)

2.2.1.1 Ensure public network access is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Disable public network access to prevent exposure to the internet and reduce the risk of unauthorized access. Use private endpoints and Azure Role-Based Access Control (RBAC) to securely manage access within trusted networks.

Rationale:

Disabling public network access improves security by ensuring that a service is not exposed on the public internet.

Impact:

Disabling public network access restricts access to the service. This enhances security but may require the configuration of private endpoints for any services or users needing access within trusted networks.

Audit:




Remediation:




Additional Information:

This Common Reference Recommendation is referenced in the following Service Recommendations:

- Storage Services > Storage Accounts > Networking > **"Ensure that 'Public Network Access' is 'Disabled' for storage accounts"**
- Storage Services > Azure Elastic SAN > **"Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN"**
- Storage Services > Azure Backup > Recovery Services Vaults > **"Ensure public network access on Recovery Services vaults is Disabled"**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>14.6 <u>Protect Information through Access Control Lists</u></p> <p>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>			

2.2.1.2 Ensure Network Access Rules are set to Deny-by-default (Automated)

Profile Applicability:

- Level 1

Description:

Restricting default network access provides a foundational level of security to networked resources. To limit access to selected networks, the default action must be changed.

Rationale:

Resources using Virtual Network interfaces should be configured to deny-by-default all access from all networks (including internet traffic). Access can be granted to traffic from specific Azure Virtual networks, allowing a secure network boundary for specific applications to be built. If necessary, access can also be granted to public internet IP address ranges to enable connections from specific internet or on-premises clients.

For all traffic inbound from- and outbound to- the internet, a NAT Gateway is recommended at minimum, and ideally all traffic flows through a security gateway device such as a firewall. Security gateway devices will provide an additional level of visibility to inbound and outbound traffic and usually perform advanced monitoring and response activity such as intrusion detection and prevention (IDP), and deep packet inspection (DPI) which help detect activity indicating vulnerabilities and threats.

Impact:

All allowed networks and protocols will need to be allow-listed which creates some administrative overhead.

Implementing a deny-by-default rule may result in a loss of network connectivity. Careful planning and a scheduled implementation window allowing for downtime is highly recommended.

Audit:

Remediation:

Default Value:

By default, interfaces attached to virtual networks will accept connections from clients on any network and have a default outbound access rule which allows access to the internet.

The default outbound access rule is scheduled for retirement on September 30th, 2025: <https://azure.microsoft.com/en-us/updates?id=default-outbound-access-for-vms-in-azure-will-be-retired-transition-to-a-new-method-of-internet-access>

References:




1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

Additional Information:

This Common Reference Recommendation is referenced in the following Service Recommendations:

- Storage Services > Storage Accounts > Networking > **"Ensure Default Network Access Rule for Storage Accounts is Set to Deny"**
-

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			

2.2.2 Private Endpoints

2.2.2.1 Ensure Private Endpoints are used to access {service} (Automated)

Profile Applicability:

- Level 2

Description:

Use private endpoints to allow clients and services to securely access data located over a network via an encrypted Private Link. To do this, the private endpoint uses an IP address from the VNet for each service. Network traffic between disparate services securely traverses encrypted over the VNet. This VNet can also link addressing space, extending your network and accessing resources on it. Similarly, it can be a tunnel through public networks to connect remote infrastructures together. This creates further security through segmenting network traffic and preventing outside sources from accessing it.

Rationale:

Securing traffic between services through encryption protects the data from easy interception and reading.

Impact:

A Private Endpoint costs approximately US\$7.30 per month. If an Azure Virtual Network is not implemented correctly, this may result in the loss of critical network traffic.

Audit:

Remediation:

Default Value:

By default, Private Endpoints are not created for services.





References:

1. <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>
2. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal>
3. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-cli?tabs=dynamic-ip>
4. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-powershell?tabs=dynamic-ip>
5. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

Additional Information:

A NAT gateway is the recommended solution for outbound internet access.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	14.1 <u>Segment the Network Based on Sensitivity</u> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			

2.2.3 Private Link

2.3 Identity and Access Management

2.4 Logging

3 Archive Storage (Reference)

Coverage Location:

- Benchmark: "CIS Microsoft Azure **Storage Services** Benchmark" (this Benchmark)
- Section: **Azure Blob Storage**

Archive Storage in Azure is an "Access tier" of Azure Blob Storage. Azure Blob Storage is a sub-type product of "Storage Accounts," so security best practice recommendations for Archive Storage will be covered in the "Azure Blob Storage" section of this Benchmark.

Resources for Archive Storage

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage>

Archive Storage service overview:

- <https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview#archive-access-tier>

4 Azure Managed Lustre

This section covers security best practice recommendations for Azure Managed Lustre.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Managed Lustre

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/managed-lustre/>

Azure Managed Lustre service overview:

- <https://learn.microsoft.com/en-us/azure/azure-managed-lustre/amlfs-overview>

Microsoft Cloud Security Baseline for Azure Managed Lustre:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-managed-lustre-security-baseline>

4.1 Ensure 'Key encryption key' is set to a customer-managed key for Azure Managed Lustre file systems (Automated)

Profile Applicability:

- Level 2

Description:

Enable customer-managed encryption keys (CMEK) for Azure Managed Lustre file systems to enhance data security and provide greater control over encryption processes. By using CMEK, organizations can manage their own encryption keys within Azure Key Vault, allowing them to rotate, revoke, or otherwise control access to these keys in accordance with their security policies.

Rationale:

Using customer-managed encryption keys (CMEK) gives organizations complete control over encryption keys, ensuring compliance and enhancing data security. CMEK allows for key rotation, revocation, and lifecycle management, thus improving data protection and facilitating immediate control over data access in Azure Managed Lustre file systems.

Impact:

There are costs and configuration overhead associated with setting up and managing customer-managed keys.

Audit:

Audit from Azure Portal

1. Go to **Azure Managed Lustre**.
2. Click the name of a file system.
3. Under **Settings**, click **Properties**.
4. Under **Encryption settings**, ensure that the value next to **Key encryption key** is **View value as JSON**.
5. Repeat steps 1-4 for each file system.

Audit from Azure CLI

Run the following command to list Azure Managed Lustre file systems:

```
az amlfs list
```

For each file system, run the following command:

```
az amlfs show --resource-group <resource-group> --name <file-system>
```

Ensure that under **encryptionSettings > keyEncryptionKey**, **keyUrl** is set to a customer-managed key URL.

Audit from PowerShell

Run the following command to install the **Az.StorageCache** module:

```
Install-Module Az.StorageCache
```

Enter **Y** when prompted.

Run the following command to list Azure Managed Lustre file systems:

```
Get-AzStorageCacheAmlFileSystem
```

Run the following command to get the file system in a resource group with a given name:

```
$filesystem = Get-AzStorageCacheAmlFileSystem -ResourceGroupName <resource-group> -Name <file-system>
```

Run the following command to get the key encryption key URL for the file system:

```
$filesystem.KeyEncryptionKeyUrl
```

Ensure that the command returns a customer-managed key URL.
Repeat for each file system.

Remediation:

To create an Azure Managed Lustre file system that uses a customer-managed encryption key:

Remediate from Azure Portal

1. Go to **Azure Managed Lustre**.
2. Click **+ Create**.
3. Provide the required information on the **Basics** tab.
4. Configure the **Advanced** tab if necessary.
5. Click the **Disk encryption keys** tab.
6. Next to **Disk encryption key type**, select the radio button next to **Customer managed**.
7. Next to **Key vault, key and version**, click **Select or create a key vault, key, or version**.
8. Select a key vault, key, and version.
9. Click **Select**.
10. Next to **User assigned identities**, click **Add user assigned managed identities**.
11. In the filter box, type to filter by identity name and/or resource group name.
12. Check the box next to a managed identity.
13. Click **Add**.
14. Click **Review + create**.
15. Click **Create**.

Remediate from Azure CLI

Run the following command to create an Azure Managed Lustre file system with a customer-managed encryption key:

```
az amlfs create --resource-group <resource-group> --name <file-system> --sku
<sku> --storage-capacity <size-in-tib> --zones [<availability-zone>] --
maintenance-window "{dayOfWeek:<day>,timeOfDayUtc:'<time>'}" --mi-user-
assigned "<user-assigned-identity-id>" --filesystem-subnet "<subnet-id>" --
encryption-setting '{"keyUrl': '<key-url>', 'sourceVault': {'id': '<key-
vault>'}}"
```

Remediate from PowerShell

Run the following command to install the **Az.StorageCache** module:

```
Install-Module Az.StorageCache
```

Enter **Y** when prompted.

Run the following command to create an Azure Manage Lustre file system with a customer-managed encryption key:

```
New-AzStorageCacheAmlFileSystem -ResourceGroupName <resource-group> -Name
<file-system> -Location <location> -MaintenanceWindowDayOfWeek '<day>' -
MaintenanceWindowTimeOfDayUtc "<time>" -FilesystemSubnet "<subnet-id>" -
SkuName "<sku>" -StorageCapacityTiB <size-in-tib> -Zone <availability-zone> -
IdentityType 'UserAssigned' -IdentityUserAssignedIdentity @"<user-assigned-
identity-id>" = @{} -KeyEncryptionKeyUrl "<key-url>" -SourceVaultId "<key-
vault>"
```

Default Value:

By default, data in Azure Managed Lustre file systems is encrypted using Microsoft-managed keys.

References:

1. <https://learn.microsoft.com/en-us/azure/azure-managed-lustre/customer-managed-encryption-keys>
2. <https://learn.microsoft.com/en-us/cli/azure/amlfs>
3. <https://learn.microsoft.com/en-us/powershell/module/az.storagecache/get-azstoragecacheamlfilesystem>
4. <https://learn.microsoft.com/en-us/powershell/module/az.storagecache/new-azstoragecacheamlfilesystem>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

5 Azure Backup

This section covers security best practice recommendations for Azure Backup.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Backup

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/backup/>

Azure Backup service overview:

- <https://learn.microsoft.com/en-us/azure/backup/backup-overview>

Microsoft Cloud Security Baseline for Azure Backup:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/backup-security-baseline>

5.1 Backup Vaults

This section covers security best practice recommendations for Backup Vaults which are a sub-product of Azure Backup.

If you would like to contribute security best practice guidance for the Azure Backup service, please join the CIS Microsoft Azure Community at <https://workbench.cisecurity.org/communities/72>.

Resources for Backup vaults

Backup vault overview:

- <https://learn.microsoft.com/en-us/azure/backup/backup-vault-overview>

5.1.1 Ensure soft delete on Backup vaults is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Soft delete provides additional protection for Backup vault data. With soft delete enabled, deleted backup data can be recovered within the retention period.

Rationale:

Important backup data could be accidentally deleted or removed by a malicious actor. With soft delete enabled, data is retained for at least 14 days before permanent deletion, allowing for the recovery of the backup data.

Impact:

There is no additional cost for backup data in the soft delete state for up to and including 14 days. However, retention beyond 14 days may incur additional charges.

Audit:

Audit from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Ensure **Soft delete** is set to **Enabled** or **Enabled with Always-On**.
5. Next to **Soft delete**, click **Update**.
6. Ensure that the **Retention period** is set to an appropriate value between 14 and 180, inclusive.
7. Repeat steps 1-6 for each Backup vault.

Audit from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault, run the following command:

```
az dataprotection backup-vault show --resource-group <resource-group> --vault-name <backup-vault>
```

Ensure that under **softDeleteSettings**, **state** is set to **on** or **alwayson**, and **retentionDurationInDays** is set to an appropriate value between 14 and 180, inclusive.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [9798d31d-6028-4dee-8643-46102185c016](#)
- **Name:** '[Preview]: Soft delete should be enabled for Backup Vaults'

Remediation:

Remediate from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Next to **Soft delete**, click **Update**.
5. Check the box next to **Soft delete**.
6. In the box next to **Retention period**, set an appropriate number of days for deleted data to be retained, between 14 and 180, inclusive.
7. If it is appropriate for your organization, check the box next to **Enable always-on soft delete**. **Note:** Once enabled, this setting cannot be disabled.
8. Click **Update**.
9. Repeat steps 1-8 for each Backup vault requiring remediation.

Remediate from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault requiring remediation, run the following command to enable soft delete and set an appropriate number of days for deleted data to be retained, between 14 and 180, inclusive:

```
az dataprotection backup-vault update --resource-group <resource-group> --vault-name <backup-vault> --soft-delete-state On --retention-duration-in-days <retention-duration>
```

Note: To enable always-on soft delete, the above command can be executed with **--soft-delete-state AlwaysOn**. Once enabled, this setting cannot be disabled.

Default Value:







Soft delete is enabled by default on newly created Backup vaults.

References:

1. <https://learn.microsoft.com/en-us/azure/backup/backup-vault-overview>

2. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-enhanced-soft-delete-about>
3. <https://learn.microsoft.com/en-us/cli/azure/dataprotection/backup-vault>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 Ensure Protection of Backups Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

5.1.2 Ensure immutability for Backup vaults is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Immutable vaults safeguard backup data by preventing any operations that could result in the loss of recovery points. The immutable vault setting can be locked, making it irreversible and preventing malicious actors from disabling it and deleting backups.

Rationale:

Enabling the immutable vault ensures that backup data is protected from unauthorized or accidental deletion. By locking the setting and making it irreversible, malicious actors are prevented from disabling the setting and deleting backups.

Impact:

There is no additional cost for enabling vault immutability; however, a vault with locked immutability cannot be deleted without contacting Azure support and will incur the standard vault costs.

Audit:

Audit from Azure Portal

1. Go to **Backup vaults**.
2. From the list of vaults, ensure that the value in the **Immutability** column for each vault is **Not locked** or **Locked**.

Audit from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault, run the following command:

```
az dataprotection backup-vault show --resource-group <resource-group> --vault-name <backup-vault>
```

Ensure that under **immutabilitySettings**, **state** is set to **Unlocked** or **Locked**.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [2514263b-bc0d-4b06-ac3e-f262c0979018](#)
- **Name:** '[Preview]: Immutability must be enabled for backup vaults'

Remediation:

Remediate from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Under the **Immutable vault** setting value, click **Settings**.
5. Check the box under **Enable vault immutability**. **Note:** It is not possible to lock immutability until immutability has been enabled.
6. Click **Apply**.
7. If it is appropriate for your organization to lock immutability, under the **Immutable vault** setting value, click **Settings**.
8. Click the toggle under **Lock immutability for this vault** to set it to **Locked**.
9. Check the box next to **Confirm locking immutability**.
10. Click **Apply**.
11. Repeat steps 1-10 for each Backup vault requiring remediation.

Remediate from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault requiring remediation, run the following command to enable vault immutability:

```
az dataprotection backup-vault update --resource-group <resource-group> --vault-name <backup-vault> --immutability-state Unlocked
```

Note: To lock the Backup vault immutability state, the above command can be executed with **--immutability-state Locked**. Once enabled, this setting cannot be disabled and it will not be possible to delete the vault.







Default Value:

Immutability is disabled by default on Backup vaults.

References:

1. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-immutable-vault-concept?tabs=backup-vault>
2. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-immutable-vault-how-to-manage?tabs=backup-vault>
3. <https://learn.microsoft.com/en-us/cli/azure/dataprotection/backup-vault>
4. <https://learn.microsoft.com/en-us/azure/backup/backup-vault-overview>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 Ensure Protection of Backups Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

5.1.3 Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Backup vaults offer two encryption options: Microsoft-managed keys, which provide automatic encryption without user intervention, and customer-managed keys (CMK), which allow organizations to retain full control over their encryption keys for enhanced security and compliance.

Rationale:

Using customer-managed keys (CMKs) to encrypt Backup vaults enhances security by granting organizations complete control over their encryption keys.

Impact:

There are costs and configuration overhead associated with setting up and managing customer-managed keys.

Audit:

Audit from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Ensure **Encryption Settings** is set to **Using 'Customer-managed keys'**.
5. Repeat steps 1-4 for each Backup vault.

Audit from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault, run the following command:

```
az dataprotection backup-vault show --resource-group <resource-group> --vault-name <backup-vault>
```

Ensure that under **properties** > **securitySettings** > **encryptionSettings** > **keyVaultProperties**, a key **keyUri** exists with the value set to a customer-managed key URI.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [d6588149-9f06-462c-a076-56aece45b5ba](#)
- **Name:** '[Preview]: Azure Backup Vaults should use customer-managed keys for encrypting backup data. Also an option to enforce Infra Encryption.'

Remediation:

Note: Once encryption is configured to use a customer-managed key, this setting cannot be reversed.

Remediate from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Under **Using 'Microsoft-managed keys'**, click **Update**.
5. Check the box next to **Use your own key**.
6. Under **Encryption key**, click the radio button next to **Enter key URI** to provide a known key URI, or click the radio button next to **Select from Key Vault** to select a key from a Key Vault.
7. If entering a key URI, provide the key URI in the text box under **Key URI**.
8. If selecting a key from a Key Vault, click **select key from Key Vault**.
 1. Select **Key vault** or **Managed HSM**.
 2. Select a key vault or managed HSM.
 3. Select a key.
 4. Click **Select**.
9. Select a managed identity to use for the encryption key.
10. Click **Update**.
11. Repeat steps 1-10 for each Backup vault.

Remediate from Azure CLI

For each Backup vault requiring remediation, run the following command to assign a customer-managed encryption key:

```
az dataprotection backup-vault update --resource-group <resource-group> --vault-name <backup-vault> --cmk-encryption-key-uri <cmk-uri> --cmk-encryption-state "Enabled" --cmk-identity-type "SystemAssigned"
```

Note: Use **--cmk-identity-type "UserAssigned" --cmk-user-assigned-identity-id <user-assigned-identity-id>** with the above command to provide a UserAssigned Identity Id.

Default Value:

By default, data in the Backup vault is encrypted using Microsoft-managed keys.




References:

1. <https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk-for-backup-vault>
2. <https://learn.microsoft.com/en-us/cli/azure/dataprotection/backup-vault>
3. <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-manage-user-assigned-managed-identities>

Additional Information:

- To enable encryption, it is necessary to grant the Backup vault the appropriate permissions to access the encryption key in the key vault. The key can be modified as needed. Refer to the following guide for details:
<https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk-for-backup-vault#assign-permissions-to-the-backup-vault-to-access-the-encryption-key-in-azure-key-vault>.
- Azure Backup uses system-assigned managed identities and user-assigned managed identities to authenticate the Backup vault to access encryption keys stored in Azure Key Vault. Refer to the following guide for details:
<https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk-for-backup-vault#enable-a-managed-identity-for-your-backup-vault>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

5.1.4 Ensure 'Use infrastructure encryption for this vault' is enabled on Backup vaults (Automated)

Profile Applicability:

- Level 2

Description:

In addition to using customer-managed keys for encryption at rest in the Backup vault, you can enable an additional layer of platform-managed infrastructure encryption. This dual-layer approach enhances the protection of your backup data.

Rationale:

Enabling infrastructure encryption on a Backup vault adds a second layer of protection to backup data, enhancing security and ensuring compliance for sensitive data storage. This dual-layer strategy reduces the risk of unauthorized access by keeping data encrypted even if one layer is compromised.

Impact:

Enabling infrastructure encryption on a backup vault does not incur additional costs; however, infrastructure encryption must be configured when creating the vault and requires customer-managed keys for encryption at rest. This recommendation is linked to **Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK)** and should be applied alongside it if you choose to implement this recommendation.

Audit:

Audit from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Under **Encryption Settings**, click **Update**.
5. Under **Infrastructure encryption**, ensure the box next to **Use infrastructure encryption for this vault** is checked.
6. Repeat steps 1-5 for each Backup vault.

Audit from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault, run the following command:

```
az dataprotection backup-vault show --resource-group <resource-group> --vault-name <backup-vault>
```

Ensure that under **properties > securitySettings > encryptionSettings**, **infrastructureEncryption** is set to **Enabled**.

Audit from PowerShell

Run the following command to list Backup vaults:

```
Get-AzDataProtectionBackupVault
```

Run the following command to get the Backup vault in a resource group with a given name:

```
$vault = Get-AzDataProtectionBackupVault -ResourceGroupName <resource-group> -VaultName <backup-vault>
```

Run the following command to get the infrastructure encryption setting for the Backup vault:

```
$vault.EncryptionSetting.CmkInfrastructureEncryption
```

Ensure that the command returns **Enabled**.

Repeat for each Backup vault.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [d6588149-9f06-462c-a076-56aece45b5ba](#)
- **Name:** '[Preview]: Azure Backup Vaults should use customer-managed keys for encrypting backup data. Also an option to enforce Infra Encryption.'

Remediation:

Remediate from Azure CLI

Run the following command to create a locally redundant Backup vault with a customer-managed encryption key and infrastructure encryption enabled:

```
az dataprotection backup-vault create --resource-group <resource-group> --vault-name <backup-vault> --location <location> --storage-setting "[{type:'LocallyRedundant',datastore-type:'VaultStore'}]" --type "UserAssigned" --user-assigned-identities '{"<user-assigned-identity-id>":{}}' --cmk-encryption-key-uri <cmk-uri> --cmk-encryption-state Enabled -cmk-identity-type "UserAssigned" --cmk-user-assigned-identity-id <cmk-user-assigned-identity-id> --cmk-infrastructure-encryption Enabled
```

Remediate from PowerShell

Run the following commands to create a locally redundant Backup vault with a customer-managed encryption key and infrastructure encryption enabled:

```

$sub = "<subscription-id>"

$storagesetting = New-AzDataProtectionBackupVaultStorageSettingObject -
DataStoreType VaultStore -Type LocallyRedundant

$userAssignedIdentity = @{
    "<user-assigned-identity-id>" = @{
        clientId = "<user-assigned-identity-client-id>"
        principalId = "<user-assigned-identity-principal-id>"
    }
}

$cmkIdentityId = "<cmk-user-assigned-identity-id>"

$cmkKeyUri = "<cmk-uri>"

New-AzDataProtectionBackupVault -SubscriptionId $sub -ResourceGroupName
<resource-group> -VaultName <backup-vault> -Location <location> -
StorageSetting $storagesetting -IdentityType UserAssigned -
UserAssignedIdentity $userAssignedIdentity -CmkEncryptionState Enabled -
CmkIdentityType UserAssigned -CmkUserAssignedIdentityId $cmkIdentityId -
CmkEncryptionKeyUri $cmkKeyUri -CmkInfrastructureEncryption Enabled

```

Default Value:

Infrastructure encryption is disabled by default on Backup vaults.

References:




1. <https://learn.microsoft.com/en-us/cli/azure/dataprotection/backup-vault>
2. <https://learn.microsoft.com/en-us/powershell/module/az.dataprotection/get-azdataprotectionbackupvault>
3. <https://learn.microsoft.com/en-us/powershell/module/az.dataprotection/new-azdataprotectionbackupvault>
4. <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-manage-user-assigned-managed-identities>

Additional Information:

Backup vaults use user-assigned managed identities to authenticate the Backup vault to access encryption keys stored in Azure Key Vault when creating the vault with a customer-managed encryption key and infrastructure encryption enabled. Refer to the following guides for details:

- <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-manage-user-assigned-managed-identities>
- <https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk-for-backup-vault>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

5.1.5 Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults (Automated)

Profile Applicability:

- Level 2

Description:

Cross region restore enables data restoration in a secondary Azure paired region, even when the primary region is fully operational. This allows organizations to conduct drills and validate regional resiliency, thereby ensuring preparedness for potential outages.

Rationale:

Enabling cross region restore facilitates proactive resilience testing and disaster recovery planning by allowing data restoration drills in a secondary region without needing a primary region outage. This capability helps organizations validate recovery processes, identify gaps in regional failover, and ensures critical data can be accessed and restored during real disruptions.

Impact:

Enabling cross region restore on a Backup vault incurs additional costs, and once it is enabled, it cannot be disabled.

- Cross region restore is an irreversible storage property.
- Cross region restore is currently supported for limited workloads.
- Cross region restore can only be enabled if the redundancy of the vault is GRS.

Audit:

Audit from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Under **Vault Settings**, ensure that **Cross Region Restore** is set to **Enabled**.
5. Repeat steps 1-4 for each Backup vault.

Audit from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault, run the following command:

```
az dataprotection backup-vault show --resource-group <resource-group> --vault-name <backup-vault>
```

Ensure that under **properties** > **featureSettings** > **crossRegionRestoreSettings**, **state** is set to **Enabled**.

Audit from PowerShell

Run the following command to list Backup vaults:

```
Get-AzDataProtectionBackupVault
```

Run the following command to get the Backup vault in a resource group with a given name:

```
$vault = Get-AzDataProtectionBackupVault -ResourceGroupName <resource-group> -VaultName <backup-vault>
```

Run the following command to get the cross region restore setting for the Backup vault:

```
$vault.CrossRegionRestoreState
```

Ensure that the command returns **Enabled**.
Repeat for each Backup vault.

Remediation:

Remediate from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Under **Vault Settings**, next to **Cross Region Restore**, click **Update**.
5. Click the toggle switch under **Cross Region Restore** to set it to **Enable**.
6. Click **Apply**.
7. Repeat steps 1-6 for each Backup vault requiring remediation.

Remediate from Azure CLI

For each Backup vault requiring remediation, run the following command to enable cross region restore:

```
az dataprotection backup-vault update --resource-group <resource-group> --vault-name <backup-vault> --cross-region-restore-state Enabled
```

Remediate from PowerShell

For each Backup vault requiring remediation, run the following command to enable cross region restore:

```
Update-AzDataProtectionBackupVault -ResourceGroupName <resource-group> -VaultName <backup-vault> -CrossRegionRestoreState Enabled
```







Default Value:

Cross region restore is disabled by default on Backup vaults.

References:

1. <https://learn.microsoft.com/en-gb/azure/backup/backup-vault-overview#cross-region-restore-support-for-postgresql-using-azure-backup>
2. <https://learn.microsoft.com/en-us/azure/backup/tutorial-cross-region-restore>
3. <https://azure.microsoft.com/en-gb/pricing/details/backup/>
4. <https://learn.microsoft.com/en-us/cli/azure/dataprotection/backup-vault>
5. <https://learn.microsoft.com/en-us/powershell/module/az.dataprotection/get-azdataprotectionbackupvault>
6. <https://learn.microsoft.com/en-us/powershell/module/az.dataprotection/update-azdataprotectionbackupvault>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 Ensure Protection of Backups Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

5.1.6 Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults (Automated)

Profile Applicability:

- Level 1

Description:

Disable cross subscription restore for Backup vaults to ensure that backup data can only be restored within the same subscription as the Backup vault, preventing restoration to targets in other subscriptions.

Rationale:

Cross subscription restores increases security risks by widening access to sensitive backup data, potentially leading to accidental or intentional exposure, unauthorized access, or data exfiltration across environments.

Impact:

Organizations may need to consider alternatives for disaster recovery scenarios, and if utilizing multiple subscriptions, may need to make adjustments or consider alternatives for data access. Costs could be incurred if alternative or additional backup infrastructure is required to account for the disabling of cross subscription restore.

Audit:

Audit from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Under **Vault Settings**, ensure that **Cross Subscription Restore** is set to **Disabled** or **Permanently Disabled**.
5. Repeat steps 1-4 for each Backup vault.

Audit from Azure CLI

Run the following command to list Backup vaults:

```
az dataprotection backup-vault list
```

For each Backup vault, run the following command:

```
az dataprotection backup-vault show --resource-group <resource-group> --vault-name <backup-vault>
```

Ensure that under **properties > featureSettings > crossSubscriptionRestoreSettings**, **state** is set to **Disabled** or **PermanentlyDisabled**.

Audit from PowerShell

Run the following command to list Backup vaults:

```
Get-AzDataProtectionBackupVault
```

Run the following command to get the Backup vault in a resource group with a given name:

```
$vault = Get-AzDataProtectionBackupVault -ResourceGroupName <resource-group>  
-VaultName <backup-vault>
```

Run the following command to get the cross subscription restore setting for the Backup vault:

```
$vault.CrossSubscriptionRestoreState
```

Ensure that the command returns **Disabled** or **PermanentlyDisabled**.
Repeat for each Backup vault.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [4d479a11-f2b5-4f0a-bb1e-d2332aa95cda](#)
- **Name:** '[Preview]: Disable Cross Subscription Restore for Backup Vaults'

Remediation:

Remediate from Azure Portal

1. Go to **Backup vaults**.
2. Click the name of a Backup vault.
3. Under **Manage**, click **Properties**.
4. Under Vault Settings, next to Cross Subscription Restore, click Update.
5. Select the radio button next to **Disable Cross Subscription Restore** or **Permanently disable Cross Subscription Restore on this vault**.
6. If selecting to permanently disable cross subscription restore, check the box next to **Are you sure you want to permanently disable Cross Subscription Restore? Once disabled, it cannot be re-enabled**.
7. Click **Update**.
8. Repeat steps 1-7 for each Backup vault requiring remediation.

Remediate from Azure CLI

For each Backup vault requiring remediation, run the following command to disable cross subscription restore:

```
az dataprotection backup-vault update --resource-group <resource-group> --vault-name <backup-vault> --cross-subscription-restore-state Disabled
```

Note: Use **--cross-subscription-restore-state PermanentlyDisabled** with the above command to permanently disable cross subscription restore.

Remediate from PowerShell

For each Backup vault requiring remediation, run the following command to disable cross subscription restore:

```
Update-AzDataProtectionBackupVault -ResourceGroupName <resource-group> -VaultName <backup-vault> -CrossSubscriptionRestoreState Disabled
```

Note: Use **-CrossSubscriptionRestoreState PermanentlyDisabled** with the above command to permanently disable cross subscription restore.

Default Value:

Cross subscription restore is enabled by default on Backup vaults.







References:

1. <https://learn.microsoft.com/en-us/cli/azure/dataprotection/backup-vault>
2. <https://learn.microsoft.com/en-us/powershell/module/az.dataprotection/get-azdataprotectionbackupvault>
3. <https://learn.microsoft.com/en-us/powershell/module/az.dataprotection/update-azdataprotectionbackupvault>
4. <https://learn.microsoft.com/en-us/azure/backup/create-manage-backup-vault#cross-subscription-restore-using-azure-portal>

Additional Information:

If cross subscription restore is permanently disabled on a vault, it cannot be re-enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

5.2 Recovery Services Vaults

This section covers security best practice recommendations for Recovery Services Vaults which are a sub-product of Azure Backup.

If you would like to contribute security best practice guidance for the Azure Backup service, please join the CIS Microsoft Azure Community at <https://workbench.cisecurity.org/communities/72>.

Resources for Recovery Services vaults

Recovery Services vault overview:

- <https://learn.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview>

5.2.1 Ensure soft delete on Recovery Services vaults is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Soft delete provides additional protection for Recovery Services vault data. With soft delete enabled, deleted backup data can be recovered within the retention period.

Rationale:

Important backup data could be accidentally deleted or removed by a malicious actor. With soft delete enabled, data is retained for at least 14 days before permanent deletion, allowing for the recovery of the backup data.

Impact:

There is no additional cost for backup data in the soft delete state for up to and including 14 days. However, retention beyond 14 days may incur additional charges.

Audit:

Audit from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Soft Delete and security settings**, click **Update**.
5. Ensure the box next to **Enable soft delete for cloud workloads** is checked.
6. Ensure the box next to **Enable soft delete and security settings for hybrid workloads** is checked.
7. Ensure that the **Soft delete retention period** is set to an appropriate value between 14 and 180, inclusive.
8. Repeat steps 1-7 for each Recovery Services vault.

Audit from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault, run the following command:

```
az backup vault show --resource-group <resource-group> --name <recovery-services-vault>
```

Ensure that under **softDeleteSettings**, **softDeleteState** is set to **Enabled**, **enhancedSecurityState** is set to **Enabled**, and **softDeleteRetentionPeriodInDays** is set to an appropriate value between 14 and 180, inclusive.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [31b8092a-36b8-434b-9af7-5ec844364148](#)
- **Name:** '[Preview]: Soft delete must be enabled for Recovery Services Vaults.'

Remediation:

Remediate from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Soft Delete and security settings**, click **Update**.
5. Check the box next to **Enable soft delete for cloud workloads**.
6. Check the box next to **Enable soft delete and security settings for hybrid workloads**.
7. In the box next to **Soft delete retention period**, set an appropriate number of days for deleted data to be retained, between 14 and 180, inclusive.
8. If it is appropriate for your organization, check the box next to **Enable always-on soft delete**. **Note:** Once enabled, this setting cannot be disabled.
9. If enabling always-on soft delete, check the box next to **Confirm enabling always-on soft delete**.
10. Click **Update**.
11. Repeat steps 1-10 for each Recovery Services vault requiring remediation.

Remediate from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault requiring remediation, run the following command to enable soft delete and set an appropriate number of days for deleted data to be retained, between 14 and 180, inclusive:

```
az backup vault backup-properties set --resource-group <resource-group> --name <recovery-services-vault> --soft-delete-feature-state Enable --hybrid-backup-security-features Enable --soft-delete-duration <retention-duration>
```

Note: To enable always-on soft delete, the above command can be executed with **--soft-delete-feature-state AlwaysOn**. Once enabled, this setting cannot be disabled.

Default Value:

Soft delete is enabled by default on newly created Recovery Services vaults.

References:







1. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview>
2. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature-cloud>
3. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-enhanced-soft-delete-about>
4. <https://learn.microsoft.com/en-us/azure/backup/soft-delete-virtual-machines>
5. <https://learn.microsoft.com/en-us/azure/backup/soft-delete-sql-saphana-in-azure-vm>
6. <https://learn.microsoft.com/en-us/cli/azure/backup/vault>

Additional Information:

Azure Backup soft delete protection is available for the following services:

- Azure virtual machines
- SQL server in Azure VM and SAP HANA in Azure VM workloads

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 <u>Establish and Maintain a Data Recovery Process</u> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 <u>Ensure Protection of Backups</u> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

5.2.2 Ensure immutability for Recovery Services vaults is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Immutable vaults safeguard backup data by preventing any operations that could result in the loss of recovery points. The immutable vault setting can be locked, making it irreversible and preventing malicious actors from disabling it and deleting backups.

Rationale:

Enabling the immutable vault ensures that backup data is protected from unauthorized or accidental deletion. By locking the setting and making it irreversible, malicious actors are prevented from disabling the setting and deleting backups.

Impact:

There is no additional cost for enabling vault immutability; however, a vault with locked immutability cannot be deleted without contacting Azure support and will incur the standard vault costs.

Audit:

Audit from Azure Portal

1. Go to **Recovery Services vaults**.
2. From the list of vaults, ensure that the value in the **Immutability** column for each vault is **Not locked** or **Locked**.

Audit from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault, run the following command:

```
az backup vault show --resource-group <resource-group> --name <recovery-services-vault>
```

Ensure that under **immutabilitySettings**, **state** is set to **Unlocked** or **Locked**.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [d6f6f560-14b7-49a4-9fc8-d2c3a9807868](#)
- **Name:** '[Preview]: Immutability must be enabled for Recovery Services vaults'

Remediation:

Remediate from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Immutable vault**, click **Settings**.
5. Check the box under **Enable vault immutability**. **Note:** It is not possible to lock immutability until immutability has been enabled.
6. Click **Apply**.
7. If it is appropriate for your organization to lock immutability, under **Immutable vault**, click **Settings**.
8. Click the toggle under **Lock immutability for this vault** to set it to **Locked**.
9. Check the box next to **Confirm locking immutability**.
10. Click **Apply**.
11. Repeat steps 1-10 for each Recovery Services vault requiring remediation.

Remediate from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault requiring remediation, run the following command to enable vault immutability:







```
az backup vault update --resource-group <resource-group> --name <recovery-services-vault> --immutability-state Unlocked
```

Note: To lock the Recovery Services vault immutability state, the above command can be executed with **--immutability-state Locked**. Once enabled, this setting cannot be disabled and it will not be possible to delete the vault.

Default Value:

Immutability is disabled by default on Recovery Services vaults.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 <u>Establish and Maintain a Data Recovery Process</u> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 <u>Ensure Protection of Backups</u> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

5.2.3 Ensure backup data in Recovery Services vaults is encrypted using customer-managed keys (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Recovery Services vaults offer two encryption options: Microsoft-managed keys, which provide automatic encryption without user intervention, and customer-managed keys (CMK), which allow organizations to retain full control over their encryption keys for enhanced security and compliance.

Rationale:

Using customer-managed keys (CMKs) to encrypt Recovery Services vaults enhances security by granting organizations complete control over their encryption keys.

Impact:

There are costs and configuration overhead associated with setting up and managing customer-managed keys.

Audit:

Audit from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Encryption Settings**, click **Update**.
5. Ensure the box next to **Use your own key** is checked, and a key URI is displayed under **Encryption key**.
6. Repeat steps 1-5 for each Recovery Services vault.

Audit from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault, run the following command:

```
az backup vault encryption show --resource-group <resource-group> --name <recovery-services-vault>
```

Ensure that under **properties**, **encryptionAtRestType** is set to **CustomerManaged**, and a key **keyUri** exists with the value set to a customer-managed key URI.

Audit from PowerShell

Run the following command to list Recovery Services vaults:

```
Get-AzRecoveryServicesVault
```

Run the following command to get the Recovery Services vault in a resource group with a given name:

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName <resource-group> -  
Name <recovery-services-vault>
```

Run the following command to get the encryption setting for the Recovery Services vault:

```
$vault.Properties.EncryptionProperty.KeyVaultProperties
```

Ensure that the command returns a customer-managed key URI.

Repeat for each Recovery Services vault.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [2e94d99a-8a36-4563-bc77-810d8893b671](#)
- **Name:** '[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data'

Remediation:

Note: Once encryption is configured to use a customer-managed key, this setting cannot be reversed.

Remediate from Azure Portall

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Encryption Settings**, click **Update**.
5. Check the box next to **Use your own key**.
6. Under **Encryption key**, click the radio button next to **Enter key URI** to provide a known key URI, or click the radio button next to **Select from Key Vault** to select a key from a Key Vault.
7. If entering a key URI, provide the key URI in the text box under **Key URI**.
8. If selecting a key from a Key Vault, click **select key from Key Vault**.
 1. Select **Key vault** or **Managed HSM**.
 2. Select a key vault or managed HSM.
 3. Select a key.
 4. Click **Select**.
9. Select a managed identity to use for the encryption key.
10. Click **Update**.

11. Repeat steps 1-10 for each Recovery Services vault.

Remediate from Azure CLI

For each Recovery Services vault requiring remediation, run the following command to assign a customer-managed encryption key:

```
az backup vault encryption update --resource-group <resource-group> --name <recovery-services-vault> --encryption-key-id <cmk-uri> --mi-system-assigned
```

Note: Use `--mi-user-assigned` with the above command to provide a UserAssigned Identity Id.

Remediate from PowerShell

For each Recovery Services vault requiring remediation, run the following command to assign a customer-managed encryption key:

```
Set-AzRecoveryServicesVaultProperty -VaultId <recovery-services-vault-id> -EncryptionKeyId <cmk-uri> -UseSystemAssignedIdentity $true
```

Note: Use `-UseSystemAssignedIdentity $false` with the above command and `-UserAssignedIdentity` to provide a UserAssigned Identity Id.

Default Value:

By default, data in the Recovery Services vault is encrypted using Microsoft-managed keys.

References:




1. <https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk>
2. <https://learn.microsoft.com/en-us/cli/azure/backup/vault>
3. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/get-azrecoveryservicesvault>
4. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/set-azrecoveryservicesvaultproperty>
5. <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-manage-user-assigned-managed-identities>

Additional Information:

- This feature can only be applied to new Recovery Services vaults. Unfortunately, vaults that currently contain existing items that are registered or have previously attempted registration are not supported.
- To enable encryption, it is necessary to grant the Recovery Services vault the appropriate permissions to access the encryption key in the key vault. The key can be modified as needed. Refer to the following guide for details: <https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk#assign-permissions-to-the-recovery-services-vault-to-access-the-encryption-key-in-azure-key-vault>.
- Azure Backup uses system-assigned managed identities and user-assigned managed identities to authenticate the Recovery Services vault to access

encryption keys stored in Azure Key Vault. Refer to the following guide for details: <https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk#enable-a-managed-identity-for-your-recovery-services-vault>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

5.2.4 Ensure 'Use infrastructure encryption for this vault' is enabled on Recovery Services vaults (Automated)

Profile Applicability:

- Level 2

Description:

In addition to using customer-managed keys for encryption at rest in the Recovery Services vault, you can enable an additional layer of platform-managed infrastructure encryption. This dual-layer approach enhances the protection of your backup data.

Rationale:

Enabling infrastructure encryption on an Azure Recovery Services vault adds a second layer of protection to backup data, enhancing security and ensuring compliance for sensitive data storage. This dual-layer strategy reduces the risk of unauthorized access by keeping data encrypted even if one layer is compromised.

Impact:

Enabling infrastructure encryption on an Azure Recovery Services vault does not incur additional costs; however infrastructure encryption must be set when configuring the encryption of the vault for the first time and requires customer-managed keys for encryption at rest. Once configured, the infrastructure encryption setting cannot be changed. This recommendation is linked to [Ensure that backup data in Recovery Services vaults is encrypted using customer-managed keys \(CMK\)](#) and should be applied alongside it if you choose to implement this recommendation.

Audit:

Audit from Azure Portal

1. Go to [Recovery Services vaults](#).
2. Click the name of a Recovery Services vault.
3. Under [Settings](#), click [Properties](#).
4. Under [Encryption Settings](#), click [Update](#).
5. Under [Infrastructure encryption](#), ensure the box next to [Use infrastructure encryption for this vault](#) is checked.
6. Repeat steps 1-5 for each Recovery Services vault.

Audit from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault, run the following command:

```
az backup vault encryption show --resource-group <resource-group> --name  
<recovery-services-vault>
```

Ensure that **infrastructureEncryptionState** is set to **Enabled**.

Audit from PowerShell

Run the following command to list Recovery Services vaults:

```
Get-AzRecoveryServicesVault
```

Run the following command to get the Recovery Services vault in a resource group with a given name:

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName <resource-group> -  
Name <recovery-services-vault>
```

Run the following command to get the infrastructure encryption setting for the Recovery Services vault:

```
$vault.Properties.EncryptionProperty.InfrastructureEncryption
```

Ensure that the command returns **Enabled**.

Repeat for each Recovery Services vault.

Remediation:

Remediate from Azure Portal

After configuring a customer-managed key for encryption, next to **Infrastructure Encryption**, click the radio button next to **Enabled**.

Remediate from Azure CLI

For each Recovery Services vault requiring remediation, run the following command to assign a customer-managed encryption key and enable infrastructure encryption:

```
az backup vault encryption update --resource-group <resource-group> --name  
<recovery-services-vault> --encryption-key-id <cmk-uri> --mi-system-assigned  
--infrastructure-encryption Enabled
```

Note: Use **--mi-user-assigned** with the above command to provide a UserAssigned Identity Id.

Remediate from PowerShell

For each Recovery Services vault requiring remediation, run the following command to assign a customer-managed encryption key and enable infrastructure encryption:

```
Set-AzRecoveryServicesVaultProperty -VaultId <recovery-services-vault-id> -  
EncryptionKeyId <cmk-uri> -UseSystemAssignedIdentity $true -  
InfrastructureEncryption
```

Note: Use **-UseSystemAssignedIdentity \$false** with the above command and **-UserAssignedIdentity** to provide a UserAssigned Identity Id.




Default Value:

Infrastructure encryption is disabled by default on Azure Recovery Services vaults.

References:

1. <https://learn.microsoft.com/en-us/azure/backup/backup-encryption>
2. <https://learn.microsoft.com/en-us/cli/azure/backup/vault/encryption>
3. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/get-azrecoveryservicesvault>
4. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/set-azrecoveryservicesvaultproperty>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

5.2.5 Ensure public network access on Recovery Services vaults is Disabled (Automated)

Profile Applicability:

- Level 1

Description:

Disable public network access on Recovery Services vaults to prevent exposure to the internet and reduce the risk of unauthorized access. Use private endpoints and Azure Role-Based Access Control (RBAC) to securely manage access within trusted networks.

Rationale:

Disabling public network access improves security by ensuring that a Recovery Services vault is not exposed on the public internet.

Impact:

Disabling public network access on Recovery Services vaults restricts access to the vault. This enhances security but may require the configuration of private endpoints for any services or users needing access within trusted networks.

Audit:

Audit from Azure Portal

1. Go to **Recovery Services** vaults.
2. Click the name of a vault.
3. Under **Settings**, click **Networking**.
4. Under **Public access**, ensure that **Public network access** is set to **Deny**.
5. Repeat steps 1-4 for each Recovery Services vault.

Audit from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault, run the following command:

```
az backup vault show --resource-group <resource-group> --name <recovery-services-vault>
```

Ensure that under **properties**, **publicNetworkAccess** is set to **Disabled**.

Audit from PowerShell

Run the following command to list Recovery Services vaults:

```
Get-AzRecoveryServicesVault
```

Run the following command to get the vault in a resource group with a given name:

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName <resource-group> -  
Name <recovery-services-vault>
```

Run the following command to get the public network access setting for the vault:

```
$vault.Properties.PublicNetworkAccess
```

Ensure that the command returns **Disabled**.

Repeat for each Recovery Services vault.

Remediation:

Remediate from Azure Portal

1. Go to **Recovery Services** vaults.
2. Click the name of a vault.
3. Under **Settings**, click **Networking**.
4. Under **Public access**, click the radio button next to **Deny**.
5. Click **Apply**.
6. Repeat steps 1-5 for each Recovery Services vault requiring remediation.

Remediate from Azure CLI

For each Recovery Services vault requiring remediation, run the following command to disable public network access:

```
az backup vault update --resource-group <resource-group> --name <recovery-  
services-vault> --public-network-access Disable
```

Remediate from PowerShell

For each Recovery Services vault requiring remediation, run the following command to disable public network access:

```
Update-AzRecoveryServicesVault -ResourceGroupName <resource-group> -Name  
<recovery-services-vault> -PublicNetworkAccess "Disabled"
```

Default Value:

Public network access is enabled by default on Recovery Services vaults.

References:

1. <https://learn.microsoft.com/en-us/azure/backup/private-endpoints#deny-public-network-access-to-the-vault>
2. <https://learn.microsoft.com/en-us/cli/azure/backup/vault?view=azure-cli-latest#az-backup-vault-list>







3. <https://learn.microsoft.com/en-us/cli/azure/backup/vault?view=azure-cli-latest#az-backup-vault-show>
4. <https://learn.microsoft.com/en-us/cli/azure/backup/vault?view=azure-cli-latest#az-backup-vault-update>
5. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/get-azrecoveryservicesvault?view=azps-12.4.0>
6. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/update-azrecoveryservicesvault?view=azps-12.4.0>

Additional Information:

Private endpoints for Backup can be only created for Recovery Services vaults that don't have any items protected to it. Azure recommends creating a new vault, and outlines a recommended workflow for disabling public network access and creating private endpoints in the following guides:

- [Create and use private endpoints \(v1 experience\) for Azure Backup](#)
- [Create and use private endpoints \(v2 experience\) for Azure Backup](#)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

5.2.6 Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults (Automated)

Profile Applicability:

- Level 2

Description:

Cross region restore enables data restoration in a secondary Azure paired region, even when the primary region is fully operational. This allows organizations to conduct drills and validate regional resiliency, thereby ensuring preparedness for potential outages.

Rationale:

Enabling cross region restore facilitates proactive resilience testing and disaster recovery planning by allowing data restoration drills in a secondary region without needing a primary region outage. This capability helps organizations validate recovery processes, identify gaps in regional failover, and ensures critical data can be accessed and restored during real disruptions.

Impact:

Enabling cross region restore on a Recovery Services vault incurs additional costs, and once it is enabled, it cannot be disabled.

- Cross region restore can only be enabled on Recovery Services vaults using the GRS replication type.
- Cross region restore is available for Azure Virtual Machines, SQL/SAP HANA databases running inside Azure VMs, and Recovery Services Agent (Preview) in the vault. There is no support for classic VMs.
- Cross region restore is currently an irreversible storage property.
- When cross region restore is enabled, Azure upgrades backup storage from GRS to read-access geo-redundant storage (RA-GRS). Pricing is updated accordingly.

Audit:

Audit from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Backup Configuration**, click **Update**.
5. Next to **Cross Region Restore**, ensure the radio button next to **Enabled** is selected.
6. Repeat steps 1-5 for each Recovery Services vault.

Audit from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault, run the following command:

```
az backup vault show --resource-group <resource-group> --name <recovery-services-vault>
```

Ensure that under **properties > redundancySettings**, **crossRegionRestore** is set to **Enabled**.

Audit from PowerShell

Run the following command to list Recovery Services vaults:

```
Get-AzRecoveryServicesVault
```

Run the following command to get the Recovery Services vault in a resource group with a given name:

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName <resource-group> -Name <recovery-services-vault>
```

Run the following command to get the cross region restore setting for the Recovery Services vault:

```
$vault.Properties.RedundancySettings.CrossRegionRestore
```

Ensure that the command returns **Enabled**.

Repeat for each Recovery Services vault.

Remediation:

Remediate from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Backup Configuration**, click **Update**.
5. Next to **Cross Region Restore**, select the radio button next to **Enabled**.
6. Click **Apply**.
7. Repeat steps 1-6 for each Recovery Services vault requiring remediation.

Remediate from Azure CLI

For each Recovery Services vault requiring remediation, run the following command to enable cross region restore:

```
az backup vault update --resource-group <resource-group> --name <recovery-services-vault> --cross-region-restore-flag Enabled
```

Remediate from PowerShell

Run the following command to get the Recovery Services vault in a resource group with a given name:

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName <resource-group> -Name <recovery-services-vault>
```

Run the following command to enable cross region restore:

```
Set-AzRecoveryServicesBackupProperty -Vault $vault -EnableCrossRegionRestore
```

Repeat for each Recovery Services vault requiring remediation.







Default Value:

Cross region restore is disabled by default on Recovery Services vaults.

References:

1. <https://learn.microsoft.com/en-us/azure/backup/backup-create-recovery-services-vault#set-cross-region-restore>
2. <https://learn.microsoft.com/en-us/cli/azure/backup/vault>
3. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/get-azrecoveryservicesvault>
4. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/set-azrecoveryservicesbackupproperty>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 Ensure Protection of Backups Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

5.2.7 Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults (Automated)

Profile Applicability:

- Level 1

Description:

Disable cross subscription restore for Recovery Services vaults to ensure that backup data can only be restored within the same subscription as the Recovery Services vault, preventing restoration to targets in other subscriptions.

Rationale:

Cross subscription restores increases security risks by widening access to sensitive backup data, potentially leading to accidental or intentional exposure, unauthorized access, or data exfiltration across environments.

Impact:

Organizations may need to consider alternatives for disaster recovery scenarios, and if utilizing multiple subscriptions, may need to make adjustments or consider alternatives for data access. Costs could be incurred if alternative or additional backup infrastructure is required to account for the disabling of cross subscription restore.

Audit:

Audit from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Cross Subscription Restore**, click **Update**.
5. Ensure that **Disable Cross Subscription Restore** or **Permanently disable Cross Subscription Restore on this vault** is selected.
6. Repeat steps 1-5 for each Recovery Services vault.

Audit from Azure CLI

Run the following command to list Recovery Services vaults:

```
az backup vault list
```

For each Recovery Services vault, run the following command:

```
az backup vault show --resource-group <resource-group> --name <recovery-services-vault>
```

Ensure that under **properties > restoreSettings > crossSubscriptionRestoreSettings**, **crossSubscriptionRestoreState** is set to **Disabled** or **PermanentlyDisabled**.

Audit from PowerShell

Run the following command to list Recovery Services vaults:

```
Get-AzRecoveryServicesVault
```

Run the following command to get the Recovery Services vault in a resource group with a given name:

```
$vault = Get-AzRecoveryServicesVault -ResourceGroupName <resource-group> -  
Name <recovery-services-vault>
```

Run the following command to get the cross subscription restore setting for the Recovery Services vault:

```
$vault.Properties.RestoreSettings.CrossSubscriptionRestoreSettings.CrossSubsc  
riptionRestoreState
```

Ensure that the command returns **Disabled** or **PermanentlyDisabled**.
Repeat for each Recovery Services vault.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [f19b0c83-716f-4b81-85e3-2dbf057c35d6](#)
- **Name:** '[Preview]: Disable Cross Subscription Restore for Azure Recovery Services vaults'

Remediation:

Remediate from Azure Portal

1. Go to **Recovery Services vaults**.
2. Click the name of a Recovery Services vault.
3. Under **Settings**, click **Properties**.
4. Under **Cross Subscription Restore**, click **Update**.
5. Select the radio button next to **Disable Cross Subscription Restore** or **Permanently disable Cross Subscription Restore on this vault**.
6. If selecting to permanently disable cross subscription restore, check the box next to **Are you sure you want to permanently disable Cross Subscription Restore? Once disabled, it cannot be re-enabled**.
7. Click **Update**.
8. Repeat steps 1-7 for each Recovery Services vault requiring remediation.

Remediate from Azure CLI

For each Recovery Services vault requiring remediation, run the following command to disable cross subscription restore:

```
az backup vault update --resource-group <resource-group> --name <recovery-services-vault> --cross-subscription-restore-state Disable
```

Note: Use **--cross-subscription-restore-state PermanentlyDisable** with the above command to permanently disable cross subscription restore.

Remediate from PowerShell

For each Recovery Services vault requiring remediation, run the following command to disable cross subscription restore:

```
Update-AzRecoveryServicesVault -ResourceGroupName <resource-group> -Name <rescovery-services-vault> -CrossSubscriptionRestoreState Disabled
```

Note: Use **-CrossSubscriptionRestoreState PermanentlyDisabled** with the above command to permanently disable cross subscription restore.

Default Value:

Cross subscription restore is enabled by default on Recovery Services vaults.







References:

1. <https://learn.microsoft.com/en-us/cli/azure/backup/vault>
2. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/get-azrecoveryservicesvault>
3. <https://learn.microsoft.com/en-us/powershell/module/az.recoveryservices/update-azrecoveryservicesvault>
4. <https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms#cross-subscription-restore-for-azure-vm>

Additional Information:

If cross subscription restore is permanently disabled on a vault, it cannot be re-enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

6 Azure Data Lake Storage (Reference)

Coverage Location:

- Benchmark: "CIS Microsoft Azure **Storage Services** Benchmark" (this benchmark)
- Section: **Azure Blob Storage**

Azure Data Lake Storage is a collection of features built on Azure Blob Storage. Azure Blob Storage is a sub-type product of "Storage Accounts," so security best practice recommendations for Azure Data Lake Storage will be covered in the "Azure Blob Storage" section of this Benchmark.

Resources for Azure Data Lake Storage

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage/data-lake-storage/>

Azure Data Lake Storage service overview:

- <https://learn.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction>

7 Azure Data Share

No prescriptive guidance exists yet for Azure Data Share.

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Data Share

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/data-share/>

Azure Data Share:

- <https://learn.microsoft.com/en-us/azure/data-share/overview>

Microsoft Cloud Security Baseline for Azure Data Share:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-data-share-security-baseline>

8 Azure Files

This section covers security best practice recommendations for Azure Files.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Files

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage/files/>

Azure Files service overview:

- <https://learn.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

Microsoft Cloud Security Baseline for Azure File Sync:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-file-sync-security-baseline>

8.1 Ensure soft delete for Azure File Shares is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Azure Files offers soft delete for file shares, allowing you to easily recover your data when it is mistakenly deleted by an application or another storage account user.

Rationale:

Important data could be accidentally deleted or removed by a malicious actor. With soft delete enabled, the data is retained for the defined retention period before permanent deletion, allowing for recovery of the data.

Impact:

When a file share is soft-deleted, the used portion of the storage is charged for the indicated soft-deleted period. All other meters are not charged unless the share is restored.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account with file shares, under **Data storage**, click on **File shares**.
3. Under **File share settings**, ensure the value for **Soft delete** shows a number of days between 1 and 365, inclusive.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

Run the following command to determine if a storage account has file shares:

```
az storage share list --account-name <storage-account>
```

For each storage account with file shares, run the following command:

```
az storage account file-service-properties show --resource-group <resource-group> --account-name <storage-account>
```

Ensure that under **shareDeleteRetentionPolicy**, **enabled** is set to **true**, and **days** is set to an appropriate value between 1 and 365, inclusive.

Audit from PowerShell

Run the following command to list storage accounts:

```
Get-AzStorageAccount -ResourceGroupName <resource-group>
```

With a storage account context set, run the following command to determine if a storage account has file shares:

```
Get-AzStorageShare
```

For each storage account with file shares, run the following command:

```
Get-AzStorageFileServiceProperty -ResourceGroupName <resource-group> -  
AccountName <storage-account>
```

Ensure that **ShareDeleteRetentionPolicy.Enabled** is set to **True** and **ShareDeleteRetentionPolicy.Days** is set to an appropriate value between 1 and 365, inclusive.

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account with file shares, under **Data storage**, click **File shares**.
3. Under **File share settings**, click the value next to **Soft delete**.
4. Under **Soft delete for all file shares**, click the toggle to set it to **Enabled**.
5. Under **Retention policies**, set an appropriate number of days to retain soft deleted data between 1 and 365, inclusive.
6. Click **Save**.

Remediate from Azure CLI

For each storage account requiring remediation, run the following command to enable soft delete for file shares and set an appropriate number of days for deleted data to be retained, between 1 and 365, inclusive:

```
az storage account file-service-properties update --account-name <storage-  
account> --enable-delete-retention true --delete-retention-days <retention-  
days>
```

Remediate from PowerShell

For each storage account requiring remediation, run the following command to enable soft delete for file shares and set an appropriate number of days for deleted data to be retained, between 1 and 365, inclusive:

```
Update-AzStorageFileServiceProperty -ResourceGroupName <resource-group> -  
AccountName <storage-account> -EnableShareDeleteRetentionPolicy $true -  
ShareRetentionDays <retention-days>
```







Default Value:

Soft delete is enabled by default at the storage account file share setting level.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/files/storage-files-enable-soft-delete>
2. <https://learn.microsoft.com/en-us/cli/azure/storage/account/file-service-properties>
3. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstoragefileserviceproperty>
4. <https://learn.microsoft.com/en-us/powershell/module/az.storage/update-azstoragefileserviceproperty>
5. <https://learn.microsoft.com/en-us/azure/storage/files/storage-files-prevent-file-share-deletion>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 <u>Establish and Maintain a Data Recovery Process</u> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 <u>Ensure Protection of Backups</u> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

8.2 Ensure root squash for NFS file shares is configured (Automated)

Profile Applicability:

- Level 1

Description:

Permissions for NFS file shares are enforced by the client OS rather than by the Azure Files service. Root squash is an administrative security feature in NFS that prevents unauthorized root-level access to the NFS server by client machines. This functionality is an important part of protecting user data and system settings from manipulation by untrusted or compromised clients.

Rationale:

Administrators should enable root squash in environments where multiple users or systems access the NFS share, especially in scenarios where client machines are not fully trusted. By converting root users to anonymous users, root squash ensures that even if a client machine is compromised, the attacker cannot exploit root privileges to access or modify critical files on the NFS server.

Impact:

There is no additional cost associated with enabling root squash; however, there may be some minor administrative overhead involved in configuring and managing permissions with root squash enabled.

Audit:

Audit from Azure Portal

1. Go to **Storage accounts**.
2. For each storage account with NFS file shares, under **Data storage**, click **File shares**.
3. Click the name of an NFS file share.
4. Click **Properties**.
5. Under **ROOT SQUASH**, ensure that **Root Squash** is selected.
6. Repeat steps 1-5 for each NFS file share in each storage account.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

For each storage account, run the following command to list file shares:

```
az storage share list --account-name <storage-account>
```

For each file share with **"protocols": ["NFS"]**, ensure that **rootSquash** is set to **RootSquash**.

Audit from PowerShell

Run the following command to list storage accounts:

```
Get-AzStorageAccount -ResourceGroupName <resource-group>
```

For each storage account, run the following command to list file shares:

```
Get-AzRmStorageShare -ResourceGroupName <resource-group> -StorageAccountName <storage-account>
```

For each NFS file share, run the following command to get the root squash configuration:

```
Get-AzRmStorageShare -ResourceGroupName <resource-group> -StorageAccountName <storage-account> -Name <nfs-file-share> | fl -Property RootSquash
```

Ensure that **RootSquash** is set to **RootSquash**.

Remediation:

Remediate from Azure Portal

1. Go to **Storage accounts**.
2. For each storage account with NFS file shares, under **Data storage**, click **File shares**.
3. Click the name of an NFS file share.
4. Click **Properties**.
5. Under **ROOT SQUASH**, select **Root Squash** from the drop-down menu.
6. Click **Save**.
7. Repeat steps 1-6 for each NFS file share requiring remediation in each storage account.

Remediate from Azure CLI

For each NFS file share requiring remediation, run the following command to enable root squash:

```
az storage share-rm update --resource-group <resource-group> --storage-account <storage-account> --name <nfs-file-share> --root-squash RootSquash
```

Remediate from PowerShell

For each NFS file share requiring remediation, run the following command to enable root squash:

```
Update-AzRmStorageShare -ResourceGroupName <resource-group> -StorageAccountName <storage-account> -Name <nfs-file-share> -RootSquash RootSquash
```

Default Value:

Root squash is disabled by default on NFS Azure file shares.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/files/nfs-root-squash>
2. <https://learn.microsoft.com/en-us/cli/azure/storage/account>
3. <https://learn.microsoft.com/en-us/cli/azure/storage/share>
4. <https://learn.microsoft.com/en-us/cli/azure/storage/share-rm>
5. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstorageaccount>
6. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azrmstorageshare>
7. <https://learn.microsoft.com/en-us/powershell/module/az.storage/update-azrmstorageshare>







Additional Information:

There are three root squash settings:

- **No root squash:** Turn off root squashing. This option is mainly useful for diskless clients or workloads as specified by workload documentation. This is the default setting when creating a new NFS Azure file share.
- **All squash:** Map all UIDs and GIDs to the anonymous user. This is useful for shares that require read-only access by all clients.
- **Root squash:** Map requests from UID/GID 0 (root) to the anonymous UID/GID. This does not apply to any other UIDs or GIDs that might be equally sensitive, such as the user bin or group staff.

All squash may be appropriate for highly restricted environments where no client-side user (including root) should have specific privileges on the NFS file share.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

8.3 Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that SMB file shares are configured to use the latest supported SMB protocol version. Keeping the SMB protocol updated helps mitigate risks associated with older SMB versions, which may contain vulnerabilities and lack essential security controls.

Rationale:

Using the latest supported SMB protocol version enhances the security of SMB file shares by preventing the exploitation of known vulnerabilities in outdated SMB versions.

Impact:

Using the latest SMB protocol version may impact client compatibility.

Audit:

Audit from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account.
3. Under **Data storage**, click **File shares**.
4. Under **File share settings**, click the link next to **Security**.
5. Under **SMB protocol versions**, ensure that **SMB3.1.1** is the only checked protocol version.
6. Repeat steps 1-5 for each storage account.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

For each storage account, run the following command:

```
az storage account file-service-properties show --resource-group <resource-group> --account-name <storage-account>
```

Ensure that under **protocolSettings > smb, versions** is set to **SMB3.1.1**; only.

Audit from PowerShell

Run the following command to list storage accounts:

```
Get-AzStorageAccount
```

Run the following command to get the file service properties for a storage account in a resource group with a given name:

```
$storageaccountfileservice = Get-AzStorageFileServiceProperty -  
ResourceGroupName <resource-group> -AccountName <storage-account>
```

Run the following command to get the SMB protocol version setting:

```
$storageaccountfileservice.ProtocolSettings.Smb.Versions
```

Ensure that the command returns **SMB3.1.1** only.
Repeat for each storage account.

Remediation:

Remediate from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account.
3. Under **Data storage**, click **File shares**.
4. Under **File share settings**, click the link next to **Security**.
5. If **Profile** is set to **Maximum compatibility**, click the drop-down menu and select **Maximum security** or **Custom**.
6. If selecting **Custom**, under **SMB protocol versions**, uncheck the boxes next to **SMB 2.1** and **SMB 3.0**.
7. Click **Save**.
8. Repeat steps 1-7 for each storage account requiring remediation.

Remediate from Azure CLI

For each storage account requiring remediation, run the following command to set the SMB protocol version:

```
az storage account file-service-properties update --resource-group <resource-group> --account-name <storage-account> --versions SMB3.1.1
```

Remediate from PowerShell

For each storage account requiring remediation, run the following command to set the SMB protocol version:

```
Update-AzStorageFileServiceProperty -ResourceGroupName <resource-group> -  
StorageAccountName <storage-account> -SmbProtocolVersion SMB3.1.1
```





Default Value:

By default, all SMB versions are allowed.

References:

1. <https://learn.microsoft.com/en-us/azure/well-architected/service-guides/azure-files#recommendations-for-smb-file-shares>
2. <https://learn.microsoft.com/en-us/azure/storage/files/files-smb-protocol#smb-security-settings>
3. <https://learn.microsoft.com/en-us/cli/azure/storage/account/file-service-properties>
4. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstoragefileserviceproperty>
5. <https://learn.microsoft.com/en-us/powershell/module/az.storage/update-azstoragefileserviceproperty>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.6 <u>Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

8.4 Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares (Automated)

Profile Applicability:

- Level 1

Description:

Implement SMB channel encryption with AES-256-GCM for SMB file shares to ensure data confidentiality and integrity in transit. This method offers strong protection against eavesdropping and man-in-the-middle attacks, safeguarding sensitive information.

Rationale:

AES-256-GCM encryption enhances the security of data transmitted over SMB channels by safeguarding it from unauthorized interception and tampering.

Impact:

Using the AES-256-GCM SMB channel encryption may impact client compatibility.

Audit:

Audit from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account.
3. Under **Data storage**, click **File shares**.
4. Under **File share settings**, click the link next to **Security**.
5. Under **SMB channel encryption**, ensure that **AES-256-GCM**, or higher, is the only checked SMB channel encryption setting.
6. Repeat steps 1-5 for each storage account.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

For each storage account, run the following command:

```
az storage account file-service-properties show --resource-group <resource-group> --account-name <storage-account>
```

Ensure that under **protocolSettings > smb**, **channelEncryption** is set to **AES-256-GCM**; , or higher, only.

Audit from PowerShell

Run the following command to list storage accounts:

```
Get-AzStorageAccount
```

Run the following command to get the file service properties for a storage account in a resource group with a given name:

```
$storageaccountfileservice = Get-AzStorageFileServiceProperty -  
ResourceGroupName <resource-group> -AccountName <storage-account>
```

Run the following command to get the SMB channel encryption setting:

```
$storageaccountfileservice.ProtocolSettings.Smb.ChannelEncryption
```

Ensure that the command returns **AES-256-GCM**, or higher, only.
Repeat for each storage account.

Remediation:

Remediate from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account.
3. Under **Data storage**, click **File shares**.
4. Under **File share settings**, click the link next to **Security**.
5. If **Profile** is set to **Maximum compatibility**, click the drop-down menu and select **Maximum security** or **Custom**.
6. If selecting **Custom**, under **SMB channel encryption**, uncheck the boxes next to **AES-128-CCM** and **AES-128-GCM**.
7. Click **Save**.
8. Repeat steps 1-7 for each storage account requiring remediation.

Remediate from Azure CLI

For each storage account requiring remediation, run the following command to set the SMB channel encryption:

```
az storage account file-service-properties update --resource-group <resource-  
group> --account-name <storage-account> --channel-encryption AES-256-GCM
```

Remediate from PowerShell

For each storage account requiring remediation, run the following command to set the SMB channel encryption:

```
Update-AzStorageFileServiceProperty -ResourceGroupName <resource-group> -  
StorageAccountName <storage-account> -SmbChannelEncryption AES-256-GCM
```

Default Value:

By default, the following SMB channel encryption algorithms are allowed:





- AES-128-CCM
- AES-128-GCM

- AES-256-GCM

References:

1. <https://learn.microsoft.com/en-us/azure/well-architected/service-guides/azure-files#recommendations-for-smb-file-shares>
2. <https://learn.microsoft.com/en-us/azure/storage/files/files-smb-protocol?tabs=azure-portal#smb-security-settings>
3. <https://learn.microsoft.com/en-us/cli/azure/storage/account/file-service-properties>
4. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstoragefileserviceproperty>
5. <https://learn.microsoft.com/en-us/powershell/module/az.storage/update-azstoragefileserviceproperty>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

9 Azure Storage Actions (Preview)

As a "Preview" product, the Azure Storage Actions service will not receive development efforts for security best practice recommendations. Once the product is released, it may become eligible for security best practice recommendations depending on community interest, necessity, and priority.

While this service is in preview, it is still open for community-driven recommendations and discussion. If you would like to contribute guidance for the Azure Storage Actions service, please join the CIS Microsoft Azure Community at <https://workbench.cisecurity.org/communities/72>.

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Resources for Azure Storage Actions

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage-actions>

10 Azure NetApp Files

This section covers security best practice recommendations for Azure NetApp Files.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure NetApp Files

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/netapp/>

Azure NetApp Files service overview:

- <https://learn.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-introduction>

Microsoft Cloud Security Baseline for Azure NetApp Files:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-netapp-files-security-baseline>

10.1 Ensure 'Encryption key source' is set to 'Customer Managed Key' for Azure NetApp Files accounts (Automated)

Profile Applicability:

- Level 2

Description:

Customer-managed keys (CMK) for Azure NetApp Files volume encryption enable organizations to use their own keys instead of platform-managed ones, providing full control over encryption.

Rationale:

Using customer-managed keys (CMKs) to encrypt Azure NetApp Files volumes enhances security by granting organizations complete control over their encryption keys.

Impact:

There are costs and configuration overhead associated with setting up and managing customer-managed keys.

Audit:

Audit from Azure Portal

1. Go to **Azure NetApp Files**.
2. Click the name of a NetApp account.
3. Under **Azure NetApp Files**, click **Encryption**.
4. Ensure that **Encryption key source** is set to **Customer Managed Key**.
5. Repeat steps 1-4 for each NetApp Files account.

Audit from Azure CLI

Run the following command to list NetApp Files accounts:

```
az netappfiles account list
```

For each NetApp Files account, run the following command:

```
az netappfiles account show --resource-group <resource-group> --account-name <netapp-files-account>
```

Ensure that under **encryption**, **keySource** is set to **Microsoft.KeyVault**.

Audit from PowerShell

Run the following command to install the **Az.NetAppFiles** module:

```
Install-Module Az.NetAppFiles
```

Enter **Y** when prompted.

Run the following command to list NetApp Files accounts:

```
Get-AzResource | ? {$_.ResourceType -like 'Microsoft.NetApp/netAppAccounts'}  
| Format-Table
```

Run the following command to get the NetApp Files account in a resource group with a given name:

```
$netapp = Get-AzNetAppFilesAccount -ResourceGroupName <resource-group> -Name  
<netapp-files-account>
```

Run the following command to get the encryption key source for the NetApp Files account:

```
$netapp.Encryption.KeySource
```

Ensure that the command returns **Microsoft.KeyVault**.
Repeat for each NetApp Files account.

Remediation:

Remediate from Azure Portal

1. Go to **Azure NetApp Files**.
2. Click the name of a NetApp account.
3. Under **Azure NetApp Files**, click **Encryption**.
4. Next to **Encryption key source**, click the radio button next to **Customer Managed Key**.
5. Next to **Encryption key**, click the radio button next to **Enter key URI** to provide a known key URI, or click the radio button next to **Select from key vault** to select a key from a key vault.
6. If entering a key URI, provide the key URI in the text box next to **Key URI**.
7. If selecting a key from a key vault, click **Select a key vault and key**.
 1. From the drop-down menu next to **Key vault**, select a key vault.
 2. From the drop-down menu next to **Key**, select a key.
 3. Click **Select**.
8. Next to **Identity type**, click the radio button next to **System-assigned** to use a system-assigned managed identity, or click the radio button next to **User-assigned** to use a user-assigned managed identity.
9. If selecting a user-assigned managed identity, next to **User-assigned identity**, click **Select an identity**.
 1. In the filter box, type to filter by identity name and/or resource group name.
 2. Check the box next to a managed identity.
 3. Click **Add**.
10. Click **Save**.
11. Repeat steps 1-10 for each NetApp Files account.

Remediate from Azure CLI

For each NetApp Files account requiring remediation, run the following command to assign a customer-managed encryption key:

```
az netappfiles account update --resource-group <resource-group> --account-name <netapp-files-account> --key-source Microsoft.KeyVault --key-name <key-name> --key-vault-uri <key-vault-uri> --keyvault-resource-id <key-vault-resource-id> --identity-type SystemAssigned
```

Note: Use `--identity-type UserAssigned --user-assigned-identity <user-assigned-identity-id>` with the above command to provide a UserAssigned Identity Id.




Default Value:

By default, data in the NetApp Files account is encrypted using Microsoft-managed keys.

References:

1. <https://learn.microsoft.com/en-us/azure/azure-netapp-files/configure-customer-managed-keys>
2. <https://learn.microsoft.com/en-us/cli/azure/netappfiles>
3. <https://learn.microsoft.com/en-us/powershell/module/az.netappfiles/get-aznetappfilesaccount>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

11 Azure Blob Storage

This section covers security best practice recommendations for Azure Blob Storage. Azure Blob Storage is a core storage service type for Azure Storage Accounts. Azure Data Lake services depend on the Azure Blob Service.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Blob Storage

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage/blobs/>

Azure Blob Storage service overview:

- <https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blobs-overview>

Microsoft Cloud Security Baseline for Storage:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline>

11.1 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signatures (SAS) can be used to grant limited access to Azure Storage resources. When generating a SAS, it is possible to specify the allowed protocols for a request made with the SAS. It is recommended to allow requests over HTTPS only.

Rationale:

If a SAS is passed over HTTP and intercepted, an attacker performing a man-in-the-middle attack can read the SAS. Then, they can use that SAS just as the intended user could have. This can potentially compromise sensitive data or allow for data corruption by the malicious user.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

It is not possible to audit generated SAS.

Remediation:

Remediate from Azure Portal

If SAS have been created to allow HTTP and were created with a stored access policy (SAP), the SAS can be revoked by deleting the SAP or updating the SAP expiration time to a time in the past:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Containers**.
4. Click the three dots next to a container.
5. Click **Access policy**.
6. Click the three dots next to an access policy.
7. Click **Delete**.
8. Click **Save**.
9. Repeat steps 1-8 as needed to revoke SAS created with SAP.

If SAS have been created to allow HTTP and were not created with a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

When generating a SAS, the default selection for **Allowed protocols** is **HTTPS only**.





References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage>

Additional Information:

This recommendation is based on the recommendation **Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

11.2 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signature (SAS) tokens provide restricted access to Azure Storage resources (such as blobs, files, queues, or tables) for a defined time period with specific permissions. It enables users to interact with the resources without exposing account keys, offering precise control over the permitted actions (e.g., read, write) and the duration of access. To minimize security risks, SAS tokens should be configured with the shortest possible lifespan, ideally lasting no longer than an hour.

Rationale:

A short lifespan for SAS tokens is recommended to minimize the risk of unauthorized access. SAS tokens grant time-limited access to resources, and a longer duration increases the opportunity for misuse if the token is compromised. By setting a shorter lifespan, the potential for security breaches is reduced.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

Currently, SAS token expiration times cannot be audited. Until Microsoft makes the token expiration time a setting rather than a token creation parameter, this recommendation will require manual verification.

Remediation:

Remediate from Azure Portal

If SAS have been created without a short lifespan and were created with a stored access policy (SAP), the SAS can be revoked by deleting the SAP or updating the SAP expiration time to a time in the past:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Containers**.
4. Click the three dots next to a listed item.
5. Click **Access policy**.
6. Click the three dots next to an access policy.
7. Click **Delete**.
8. Click **Save**.

9. Repeat steps 1-8 as needed to revoke SAS created with SAP.

If SAS have been created without a short lifespan and were not created with a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

By default, expiration for shared access signature is set to 8 hours.






References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature>

Additional Information:

This recommendation is based on the recommendation **Ensure that shared access signature (SAS) tokens expire within an hour**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

11.3 Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled (Automated)

Profile Applicability:

- Level 1

Description:

Blobs in Azure storage accounts may contain sensitive or personal data, such as ePHI or financial information. Data that is erroneously modified or deleted by an application or a user can lead to data loss or unavailability.

It is recommended that soft delete be enabled on Azure storage accounts with blob storage to allow for the preservation and recovery of data when blobs or blob snapshots are deleted.

Rationale:

Blobs can be deleted incorrectly. An attacker or malicious user may do this deliberately in order to cause disruption. Deleting an Azure storage blob results in immediate data loss. Enabling this configuration for Azure storage accounts ensures that even if blobs are deleted from the storage account, the blobs are recoverable for a specific period of time, which is defined in the "Retention policies," ranging from 7 to 365 days.

Impact:

All soft-deleted data is billed at the same rate as active data. Additional costs may be incurred for deleted blobs until the soft delete period ends and the data is permanently removed.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each Storage Account with blob storage, under **Data management**, go to **Data protection**.
3. Ensure that **Enable soft delete for blobs** is checked.
4. Ensure that the retention period is a sufficient length for your organization.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

Run the following command to determine if a storage account has containers:

```
az storage container list --account-name <storage-account>
```

For each storage account with containers, ensure that the output of the below command contains **"enabled": true** and **days** is not **null**:

```
az storage blob service-properties delete-policy show --account-name  
<storage-account>
```

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each Storage Account with blob storage, under **Data management**, go to **Data protection**.
3. Check the box next to **Enable soft delete for blobs**.
4. Set the retention period to a sufficient length for your organization.
5. Click **Save**.

Remediate from Azure CLI

For each storage account requiring remediation, run the following command to enable soft delete for blobs:

```
az storage blob service-properties delete-policy update --days-retained  
<retention-days> --account-name <storage-account> --enable true
```







Default Value:

Soft delete for blob storage is **enabled** by default on storage accounts created via the Azure Portal, and **disabled** by default on storage accounts created via Azure CLI or PowerShell.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/blobs/soft-delete-blob-overview>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 <u>Establish and Maintain a Data Recovery Process</u> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 <u>Ensure Protection of Backups</u> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

11.4 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)

Profile Applicability:

- Level 1

Description:

Use stored access policies (SAP) when generating shared access signature (SAS) tokens in Azure to centrally manage permissions, expiration, and revocation settings for resource access. Stored access policies can be applied to blob containers, file shares, queues, and tables.

Rationale:

Stored access policies provide centralized control over SAS token access, allowing administrators to update permissions or revoke access. This approach strengthens security by reducing the risk of unauthorized access to storage resources.

Impact:

There is no cost for creating stored access policies, however there is some administrative overhead involved in managing these policies.

Audit:

It is not currently possible to retrieve a list of all generated SAS tokens to check if they were associated with a SAP during creation.

An SAS token that has been created with a SAP will contain an **si** parameter that references the stored access policy identifier associated with the SAS, e.g.

si=<stored-access-policy-identifier>.

The **si** parameter will be absent from an SAS token created without a SAP.

Remediation:

Remediate from Azure Portal

To create a SAP for a blob container:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Containers**.
4. Click the name of a container.
5. Under **Settings**, click **Access policy**.
6. Under **Stored access policies**, click **+ Add policy**.
7. Enter an **Identifier**.
8. From the **Permissions** drop-down, select appropriate permissions for the policy.
9. Set an appropriate **Start time** for the policy.

10. Set an appropriate **Expiry time** for the policy.
11. Click **OK**.
12. Click **Save**.
13. Repeat steps 1-12 as needed to create SAP.

When generating SAS, select a SAP from the **Stored access policy** drop-down. If SAS have been created without a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

By default, stored access policies are not associated with SAS. To use a stored access policy, it must be explicitly created and linked to the SAS at the time of creation.







References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas>
2. <https://learn.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy>

Additional Information:

This recommendation is based on the recommendation **Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.2 Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<u>14.6 Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

11.5 Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts (Automated)

Profile Applicability:

- Level 2

Description:

Enabling blob versioning allows for the automatic retention of previous versions of objects. With blob versioning enabled, earlier versions of a blob are accessible for data recovery in the event of modifications or deletions.

Rationale:

Blob versioning safeguards data integrity and enables recovery by retaining previous versions of stored objects, facilitating quick restoration from accidental deletion, modification, or malicious activity.

Impact:

Enabling blob versioning for a storage account creates a new version with each write operation to a blob, which can increase storage costs. To control these costs, a lifecycle management policy can be applied to automatically delete older versions.

Audit:

Audit from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account with blob storage.
3. In the **Overview** page, on the **Properties** tab, under **Blob service**, ensure **Versioning** is set to **Enabled**.
4. Repeat steps 1-3 for each storage account with blob storage.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

Run the following command to determine if a storage account has containers:

```
az storage container list --account-name <storage-account>
```

For each storage account with containers, ensure that the output of the below command contains **"isVersioningEnabled": true**:

```
az storage account blob-service-properties show --account-name <storage-account>
```

Audit from PowerShell

Run the following command to list storage accounts:

```
Get-AzStorageAccount
```

Run the following command to create an Azure Storage context for a storage account:

```
$context = New-AzStorageContext -StorageAccountName <storage-account>
```

Run the following command to list containers for the storage account:

```
Get-AzStorageContainer -Context $context
```

If the storage account has containers, run the following command to get the blob service properties of the storage account:

```
$account = Get-AzStorageBlobServiceProperty -ResourceGroupName <resource-group> -AccountName <storage-account>
```

Run the following command to get the blob versioning setting for the storage account:

```
$account.IsVersioningEnabled
```

Ensure that the command returns **True**.

Repeat for each storage account.

Remediation:

Remediate from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account with blob storage.
3. In the **Overview** page, on the **Properties** tab, under **Blob service**, click **Disabled** next to **Versioning**.
4. Under **Tracking**, check the box next to **Enable versioning for blobs**.
5. Select the radio button next to **Keep all versions** or **Delete versions after (in days)**.
6. If selecting to delete versions, enter a number of in the box after which to delete blob versions.
7. Click **Save**.
8. Repeat steps 1-7 for each storage account with blob storage.

Remediate from Azure CLI

For each storage account requiring remediation, run the following command to enable blob versioning:

```
az storage account blob-service-properties update --account-name <storage-account> --enable-versioning true
```

Remediate from PowerShell

For each storage account requiring remediation, run the following command to enable blob versioning:


```
Update-AzStorageBlobServiceProperty -ResourceGroupName <resource-group> -  
StorageAccountName <storage-account> -IsVersioningEnabled $true
```







Default Value:

Blob versioning is disabled by default on storage accounts.

References:

1. <https://learn.microsoft.com/en-us/cli/azure/storage/account>
2. <https://learn.microsoft.com/en-us/cli/azure/storage/account/blob-service-properties>
3. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstorageaccount>
4. <https://learn.microsoft.com/en-us/powershell/module/az.storage/new-azstoragecontext>
5. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstoragecontainer>
6. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstorageblobserviceproperty>
7. <https://learn.microsoft.com/en-us/powershell/module/az.storage/update-azstorageblobserviceproperty>
8. <https://learn.microsoft.com/en-us/azure/storage/blobs/versioning-overview>
9. <https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.1 Ensure Regular Automated Back Ups Ensure that all system data is automatically backed up on regular basis.			

11.6 Ensure locked immutability policies are used for containers storing business-critical blob data (Automated)

Profile Applicability:

- Level 2

Description:

Require locked immutability policies for all containers that store business-critical blob data. This measure protects the data from modifications or deletions, ensuring that critical information remains intact and unaltered, regardless of user actions or access permissions.

Rationale:

Implementing a locked immutability policy creates a Write Once, Read Many (WORM) storage model that safeguards critical data from accidental or malicious changes and deletions. Enforcing immutability minimizes data loss and tampering risks, enhancing data security and supporting regulatory requirements for data retention and integrity.

Impact:

Enforcing locked immutability policies for blob storage may increase long-term retention costs and require additional administrative effort for policy management.

Once the policy is locked, the container cannot be deleted or edited, and the storage account cannot be deleted until the retention period has elapsed.

Audit:

Audit from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account.
3. Under **Data storage**, click **Containers**.
4. Click the three dots next to a container.
5. Click **Access policy**.
6. Ensure a locked policy is listed under **Immutable blob storage**.
7. Repeat steps 1-6 for each blob container with business-critical blob data.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

Run the following command to determine if a storage account has containers:

```
az storage container list --account-name <storage-account>
```

For each container, run the following command to view immutability policies:

```
az storage container immutability-policy show --account-name <storage-account> --container <blob-container>
```

Ensure that an immutability policy is listed with **"state": "Locked"** for each blob container with business-critical blob data.

Remediation:

Remediate from Azure Portal

1. Go to **Storage accounts**.
2. Click the name of a storage account.
3. Under **Data storage**, click **Containers**.
4. Click the three dots next to a container.
5. Click **Access policy**.
6. Under **Immutable blob storage**, click **+ Add policy**.
7. From the **Policy type** drop-down, select **Legal hold** or **Time-based retention**.
8. If selecting legal hold:
 1. Provide at least one tag for the policy.
 2. Under **Allow protected append writes to**, select **None** or **Block and append blobs**.
9. If selecting time-based retention:
 1. Under **Set retention period for**, enter a number of days for retention.
 2. Check the box next to **Enable version-level immutability** if appropriate. Versioning must be enabled for this option to be available.
 3. Under **Allow protected append writes to**, select **None**, **Append blobs**, or **Block and append blobs**.
10. Click **Save**.
11. Click the three dots next to the policy.
12. Click **Lock policy**.
13. Enter **yes** to confirm.
14. Click **OK**.
15. Repeat steps 1-14 for each blob container requiring remediation.

Remediate from Azure CLI

For each blob container requiring remediation, run the following command to create an immutability policy:

```
az storage container immutability-policy create --account-name <storage-account> --container-name <blob-container> --period <retention-period-in-days>
```

For each blob container requiring remediation, run the following command to lock an immutability policy:

```
az storage container immutability-policy lock --account-name <storage-account> --container-name <blob-container> --if-match <immutability-policy-etag>
```






Default Value:

Blob immutability is disabled by default.

References:

1. <https://learn.microsoft.com/en-gb/azure/storage/blobs/immutable-storage-overview>
2. <https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-policy-configure-container-scope>
3. <https://learn.microsoft.com/en-us/cli/azure/storage/container/immutability-policy>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.7 <u>Establish and Maintain a Data Classification Scheme</u> Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	13.1 <u>Maintain an Inventory Sensitive Information</u> Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.			

12 Azure Data Box

This section covers security best practice recommendations for Azure Data Box.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Data Box

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/databox/>

Azure Data Box service overview:

- <https://learn.microsoft.com/en-us/azure/databox/data-box-overview>

Microsoft Cloud Security Baseline for Azure Data Box:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-data-box-security-baseline>

12.1 Ensure double encryption is used for Azure Data Box in high-security environments (Manual)

Profile Applicability:

- Level 2

Description:

Enabling double encryption on Azure Data Box applies an additional layer of encryption to safeguard data during physical transfer. This approach enhances confidentiality and integrity, ensuring that sensitive information remains secure against unauthorized access if the device is lost, stolen, or intercepted.

Rationale:

Double encryption ensures strong security for high-risk or regulated environments where data protection is critical. It enhances defense-in-depth and minimizes the risk of exposure, even during physical compromise in transit.

Impact:

Double encryption with Azure Data Box is available at no additional cost; however, enabling it may increase order processing and data copy times.

Audit:

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [c349d81b-9985-44ae-a8da-ff98d108ede8](#)
- **Name:** 'Azure Data Box jobs should enable double encryption for data at rest on the device'

Remediation:

Remediate from Azure Portal

When creating a new Azure Data Box order, on the **Security** page, under **Double encryption**, check the box next to **Enable double encryption for the order**.




Default Value:

Double encryption is disabled by default on Azure Data Box orders.

References:

1. <https://learn.microsoft.com/en-us/azure/security/fundamentals/double-encryption>
2. <https://learn.microsoft.com/en-us/azure/databox/data-box-security>
3. <https://learn.microsoft.com/en-us/azure/databox/data-box-deploy-ordered>
4. <https://learn.microsoft.com/en-us/powershell/module/az.databox/update-azdataboxjob>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

13 Azure Disk Storage (Reference)

Coverage Location:

- Benchmark: "CIS Microsoft Azure **Compute Services** Benchmark"
- Section: **Virtual Machines**

Azure Disk Storage is a product name for Azure managed disks. Azure managed disks provide block-level storage for Azure Virtual Machines. Managed disks are created and maintained for Azure Virtual Machines through the same administrative interface as Azure Virtual Machines, so all security best practice recommendations for managed disks ("Azure Disk Storage") will be found in the CIS Microsoft Azure Compute Services Benchmark under the Virtual Machines section.

Resources for Azure Disk Storage

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage/disks/>

Azure Disk Storage service overview:

- <https://learn.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview>

14 Azure Confidential Ledger

No specific prescriptive guidance exists yet for Azure Confidential Ledger.

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Confidential Ledger

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/azure-confidential-ledger/>

Azure Confidential Ledger service overview:

- <https://learn.microsoft.com/en-us/azure/confidential-ledger/overview>

15 Azure Elastic SAN

This section covers security best practices for Azure Elastic SAN.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:
<https://workbench.cisecurity.org/communities/72>.

Resources for Azure Elastic SAN

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage/elastic-san/>

Azure Elastic SAN service overview:

- <https://learn.microsoft.com/en-us/azure/storage/elastic-san/elastic-san-introduction>

15.1 Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN (Automated)

Profile Applicability:

- Level 2

Description:

Azure Elastic SAN is a scalable, high-performance cloud-based storage solution. Disabling public network access at the SAN level ensures that Elastic SAN resources are accessible only through private networks.

Rationale:

Disabling public network access for Azure Elastic SAN at the SAN level enhances security by preventing unauthorized external access to sensitive storage resources.

Impact:

Disabling public network access at the SAN level incurs no direct cost. However, there may be costs and configuration overhead associated with setting up and managing private network access to securely connect to Azure Elastic SAN resources.

Audit:

Audit from Azure Portal

1. Go to **Elastic SANs**.
2. Click the name of an Elastic SAN.
3. Under **Settings**, click **Networking**.
4. Ensure that **Public network access** is set to **Disabled**.
5. Repeat steps 1-4 for each Elastic SAN.

Audit from Azure CLI

Run the following command to list Elastic SANs:

```
az elastic-san list
```

For each Elastic SAN, run the following command:

```
az elastic-san show --resource-group <resource-group> --name <elastic-san>
```

Ensure that **publicNetworkAccess** is set to **Disabled**.

Audit from PowerShell

Run the following command to list Elastic SANs:

```
Get-AzElasticSan
```

Run the following command to get the Elastic SAN in a resource group with a given name:

```
$elasticsan = Get-AzElasticSan -ResourceGroupName <resource-group> -Name  
<elastic-san>
```

Run the following command to get the public network access setting for the Elastic SAN:

```
$elasticsan.PublicNetworkAccess
```

Ensure that the command returns **Disabled**.

Remediation:

Remediate from Azure Portal

1. Go to **Elastic SANs**.
2. Click the name of an Elastic SAN.
3. Under **Settings**, click **Networking**.
4. Under **Public network access**, click the radio button next to **Disabled**.
5. Click **Apply**.
6. Repeat steps 1-5 for each Elastic SAN.

Remediate from Azure CLI

For each Elastic SAN requiring remediation, run the following command to disable public network access:

```
az elastic-san update --resource-group <resource-group> --name <elastic-san>  
--public-network-access Disabled
```

Remediate from PowerShell

For each Elastic SAN requiring remediation, run the following command to disable public network access:

```
Update-AzElasticSan -ResourceGroupName <resource-group> -Name <elastic-san> -  
PublicNetworkAccess Disabled
```







Default Value:

Public network access at the SAN level is enabled by default, but access to individual volume groups is denied unless explicitly configured.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/elastic-san/elastic-san-networking>
2. <https://learn.microsoft.com/en-us/cli/azure/elastic-san>
3. <https://learn.microsoft.com/en-us/powershell/module/az.elasticsan/get-azelasticsan>
4. <https://learn.microsoft.com/en-us/powershell/module/az.elasticsan/update-azelasticsan>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

15.2 Ensure customer-managed keys (CMK) are used to encrypt data at rest on Azure Elastic SAN volume groups (Automated)

Profile Applicability:

- Level 2

Description:

Azure Elastic SAN volume groups offer two encryption options: Microsoft-managed keys, which provide automatic encryption without user intervention, and customer-managed keys (CMK), which allow organizations to retain full control over their encryption keys for enhanced security and compliance.

Rationale:

Using customer-managed keys (CMKs) to encrypt Azure Elastic SAN volume groups enhances security by granting organizations complete control over their encryption keys.

Impact:

There are costs and configuration overhead associated with setting up and managing customer-managed keys.

Audit:

Audit from Azure Portal

1. Go to **Elastic SANs**.
2. Click the name of an Elastic SAN.
3. Under **SAN Management**, click **Volume groups**.
4. For each volume group, ensure that the value in the **Encryption type** column is not **Platform-managed key**.

Audit from Azure CLI

Run the following command to list Elastic SANs:

```
az elastic-san list
```

For each Elastic SAN with a **volumeGroupCount** greater than 0, run the following command to list volume groups:

```
az elastic-san volume-group list --resource-group <resource-group> --elastic-san <elastic-san>
```

Ensure that for each volume group, **encryption** is set to **EncryptionAtRestWithCustomerManagedKey**.

Audit from PowerShell

Run the following command to list Elastic SANs:

```
Get-AzElasticSan
```

For each Elastic SAN with a **VolumeGroupCount** greater than 0, run the following command to list volume groups:

```
Get-AzElasticSanVolumeGroup -ResourceGroupName <resource-group> -  
ElasticSanName <elastic-san>
```

Ensure that for each volume group, **Encryption** is set to **EncryptionAtRestWithCustomerManagedKey**.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [7698f4ed-80ce-4e13-b408-ee135fa400a5](#)
- **Name:** 'ElasticSan Volume Group should use customer-managed keys to encrypt data at rest'

Remediation:

Remediate from Azure Portal

It is not currently possible to remediate from Azure Portal. Refer to the **Remediate from Azure CLI** and **Remediate from PowerShell** sections for remediation options.

Remediate from Azure CLI

For each volume group requiring remediation, run the following command to assign an identity:

```
az elastic-san volume-group update --resource-group <resource-group> --  
elastic-san <elastic-san> --volume-group <volume-group> --identity  
"{type:SystemAssigned}"
```

Note: Use **--identity '{type:UserAssigned,user-assigned-identity:"<user-assigned-identity-id>"}'** with the above command to provide a UserAssigned Identity Id.

For each volume group requiring remediation, run the following command to assign a customer-managed encryption key:

```
az elastic-san volume-group update --resource-group <resource-group> --  
elastic-san <elastic-san> --volume-group <volume-group> --encryption  
EncryptionAtRestWithCustomerManagedKey --encryption-properties "{key-vault-  
properties:{key-name:'<key>',key-vault-uri:'<key-vault-uri>'}}"
```


Remediate from PowerShell

For each volume group requiring remediation, run the following command to assign an identity:

```
Update-AzElasticSanVolumeGroup -ResourceGroupName <resource-group> -  
ElasticSanName <elastic-san> -VolumeGroupName <volume-group> -IdentityType  
SystemAssigned
```

Note: Use **-IdentityType UserAssigned -IdentityUserAssignedIdentityId <user-assigned-identity-id>** with the above command to provide a UserAssigned Identity Id.

For each volume group requiring remediation, run the following command to assign a customer-managed encryption key:

```
Update-AzElasticSanVolumeGroup -ResourceGroupName <resource-group> -  
ElasticSanName <elastic-san> -VolumeGroupName <volume-group> -Encryption  
EncryptionAtRestWithCustomerManagedKey -KeyName <key> -KeyVaultUri <key-  
vault-uri>
```

Default Value:

By default, Azure Elastic SAN volume groups are encrypted using Microsoft-managed keys.




References:

1. <https://learn.microsoft.com/en-us/azure/storage/elastic-san/elastic-san-configure-customer-managed-keys>
2. <https://learn.microsoft.com/en-us/cli/azure/elastic-san/volume-group>
3. <https://learn.microsoft.com/en-us/powershell/module/az.elasticsan/get-azelasticsanvolumegroup>
4. <https://learn.microsoft.com/en-us/powershell/module/az.elasticsan/update-azelasticsanvolumegroup>
5. <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/how-manage-user-assigned-managed-identities>

Additional Information:

- To enable encryption, it is necessary to grant the volume group the appropriate permissions to access the encryption key in the key vault. The key can be modified as needed. Refer to the following guide for details: <https://learn.microsoft.com/en-us/azure/storage/elastic-san/elastic-san-configure-customer-managed-keys?#configure-the-key-vault>.
- Azure Elastic SAN uses system-assigned managed identities and user-assigned managed identities to authenticate the volume groups to access encryption keys stored in Azure Key Vault. Refer to the following guide for details: <https://learn.microsoft.com/en-us/azure/storage/elastic-san/elastic-san-configure-customer-managed-keys#choose-a-managed-identity-to-authorize-access-to-the-key-vault>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

16 Queue Storage

This section covers security best practices for Azure Queue Storage.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:

<https://workbench.cisecurity.org/communities/72>.

Resources for Queue Storage

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage/queues/>

Queue Storage service overview:

- <https://learn.microsoft.com/en-us/azure/storage/queues/storage-queues-introduction>

Microsoft Cloud Security Baseline for Storage:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline>

16.1 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signatures (SAS) can be used to grant limited access to Azure Storage resources. When generating a SAS, it is possible to specify the allowed protocols for a request made with the SAS. It is recommended to allow requests over HTTPS only.

Rationale:

If a SAS is passed over HTTP and intercepted, an attacker performing a man-in-the-middle attack can read the SAS. Then, they can use that SAS just as the intended user could have. This can potentially compromise sensitive data or allow for data corruption by the malicious user.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

It is not possible to audit generated SAS.

Remediation:

Remediate from Azure Portal

If SAS have been created to allow HTTP and were created with a stored access policy (SAP), the SAS can be revoked by deleting the SAP or updating the SAP expiration time to a time in the past:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Queues**.
4. Click the three dots next to a queue.
5. Click **Access policy**.
6. Click the three dots next to an access policy.
7. Click **Delete**.
8. Click **Save**.
9. Repeat steps 1-8 as needed to revoke SAS created with SAP.

If SAS have been created to allow HTTP and were not created with a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

When generating a SAS, the default selection for **Allowed protocols** is **HTTPS only**.





References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage>

Additional Information:

This recommendation is based on the recommendation **Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

16.2 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signature (SAS) tokens provide restricted access to Azure Storage resources (such as blobs, files, queues, or tables) for a defined time period with specific permissions. It enables users to interact with the resources without exposing account keys, offering precise control over the permitted actions (e.g., read, write) and the duration of access. To minimize security risks, SAS tokens should be configured with the shortest possible lifespan, ideally lasting no longer than an hour.

Rationale:

A short lifespan for SAS tokens is recommended to minimize the risk of unauthorized access. SAS tokens grant time-limited access to resources, and a longer duration increases the opportunity for misuse if the token is compromised. By setting a shorter lifespan, the potential for security breaches is reduced.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

Currently, SAS token expiration times cannot be audited. Until Microsoft makes the token expiration time a setting rather than a token creation parameter, this recommendation will require manual verification.

Remediation:

Remediate from Azure Portal

If SAS have been created without a short lifespan and were created with a stored access policy (SAP), the SAS can be revoked by deleting the SAP or updating the SAP expiration time to a time in the past:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Queues**.
4. Click the three dots next to a listed item.
5. Click **Access policy**.
6. Click the three dots next to an access policy.
7. Click **Delete**.
8. Click **Save**.

9. Repeat steps 1-8 as needed to revoke SAS created with SAP.

If SAS have been created without a short lifespan and were not created with a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

By default, expiration for shared access signature is set to 8 hours.






References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature>

Additional Information:

This recommendation is based on the recommendation **Ensure that shared access signature (SAS) tokens expire within an hour**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

16.3 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)

Profile Applicability:

- Level 1

Description:

Use stored access policies (SAP) when generating shared access signature (SAS) tokens in Azure to centrally manage permissions, expiration, and revocation settings for resource access. Stored access policies can be applied to blob containers, file shares, queues, and tables.

Rationale:

Stored access policies provide centralized control over SAS token access, allowing administrators to update permissions or revoke access. This approach strengthens security by reducing the risk of unauthorized access to storage resources.

Impact:

There is no cost for creating stored access policies, however there is some administrative overhead involved in managing these policies.

Audit:

It is not currently possible to retrieve a list of all generated SAS tokens to check if they were associated with a SAP during creation.

An SAS token that has been created with a SAP will contain an **si** parameter that references the stored access policy identifier associated with the SAS, e.g.

si=<stored-access-policy-identifier>.

The **si** parameter will be absent from an SAS token created without a SAP.

Remediation:

Remediate from Azure Portal

To create a SAP for a queue:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Queues**.
4. Click the name of a queue.
5. Under **Settings**, click **Access policy**.
6. Under **Stored access policies**, click **+ Add policy**.
7. Enter an **Identifier**.
8. From the **Permissions** drop-down, select appropriate permissions for the policy.
9. Set an appropriate **Start time** for the policy.

10. Set an appropriate **Expiry time** for the policy.
11. Click **OK**.
12. Click **Save**.
13. Repeat steps 1-12 as needed to create SAP.

When generating SAS, select a SAP from the **Stored access policy** drop-down. If SAS have been created without a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

By default, stored access policies are not associated with SAS. To use a stored access policy, it must be explicitly created and linked to the SAS at the time of creation.







References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas>
2. <https://learn.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy>

Additional Information:

This recommendation is based on the recommendation **Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.2 Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<u>14.6 Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

17 Storage Accounts

This section covers security best practice recommendations for Storage Accounts in Azure.

The recommendations in this section apply to the Storage Account, but not to the Storage Services which may be running on that account. Use the Storage Account recommendations as a starting place for securing the account, then proceed to apply the recommendations from the storage services section(s) that are relevant to the storage services running on your account.

Storage Accounts are a family of account types that support different Storage Services. The Storage Account types and their supported services follow:

- **Standard general-purpose v2** supported services: Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files.
- **Premium block blobs** supported services: Blob Storage (including Data Lake Storage)
- **Premium file shares** supported services: Azure Files
- **Premium page blobs** supported services: Page blobs only

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:

<https://workbench.cisecurity.org/communities/72>.

Resources for Storage Accounts

Azure Product page:

- <https://azure.microsoft.com/en-us/products/category/storage/>

Azure Storage Account overview:

- <https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview>

Microsoft Cloud Security Baseline for Storage:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline>

17.1 Secrets and Keys

17.1.1 Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)

Profile Applicability:

- Level 1

Description:

Access Keys authenticate application access requests to data contained in Storage Accounts. A periodic rotation of these keys is recommended to ensure that potentially compromised keys cannot result in a long-term exploitable credential. The "Rotation Reminder" is an automatic reminder feature for a manual procedure.

Rationale:

Reminders such as those generated by this recommendation will help maintain a regular and healthy cadence for activities which improve the overall efficacy of a security program.

Cryptographic key rotation periods will vary depending on your organization's security requirements and the type of data which is being stored in the Storage Account. For example, PCI DSS mandates that cryptographic keys be replaced or rotated 'regularly,' and advises that keys for static data stores be rotated every 'few months.'

For the purposes of this recommendation, 90 days will be prescribed for the reminder. Review and adjustment of the 90 day period is recommended, and may even be necessary. Your organization's security requirements should dictate the appropriate setting.

Impact:

This recommendation only creates a periodic reminder to regenerate access keys. Regenerating access keys can affect services in Azure as well as the organization's applications that are dependent on the storage account. All clients that use the access key to access the storage account must be updated to use the new key.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**
2. For each Storage Account, under **Security + networking**, go to **Access keys**
3. If the button **Edit rotation reminder** is displayed, the Storage Account is compliant. Click **Edit rotation reminder** and review the **Remind me every** field for a desirable periodic setting that fits your security program's needs. If the button **Set rotation reminder** is displayed, the Storage Account is not compliant.

Audit from Powershell

```
$rgName = <resource group name for the storage>
$accountName = <storage account name>
$account = Get-AzStorageAccount -ResourceGroupName $rgName -Name $accountName

Write-Output $accountName ->
Write-Output "Expiration Reminder set to:
$(($account.KeyPolicy.KeyExpirationPeriodInDays) Days"
Write-Output "Key1 Last Rotated:
$(($account.KeyCreationTime.Key1.ToShortDateString()))"
Write-Output "Key2 Last Rotated:
$(($account.KeyCreationTime.Key2.ToShortDateString()))"
```

Key rotation is recommended if the creation date for any key is empty.
If the reminder is set, the period in days will be returned. The recommended period is 90 days.

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**
2. For each Storage Account that is not compliant, under **Security + networking**, go to **Access keys**
3. Click **Set rotation reminder**
4. Check **Enable key rotation reminders**
5. In the **Send reminders** field select **Custom**, then set the **Remind me every** field to **90** and the period drop down to **Days**
6. Click **Save**

Remediate from Powershell

```
$rgName = <resource group name for the storage>
$accountName = <storage account name>
$account = Get-AzStorageAccount -ResourceGroupName $rgName -Name $accountName
if ($account.KeyCreationTime.Key1 -eq $null -or $account.KeyCreationTime.Key2 -eq $null){
    Write-output ("You must regenerate both keys at least once before setting expiration policy")
} else {
    $account = Set-AzStorageAccount -ResourceGroupName $rgName -Name $accountName -KeyExpirationPeriodInDay 90
}
$account.KeyPolicy.KeyExpirationPeriodInDays
```






Default Value:

By default, Key rotation reminders is not configured.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-create-storage-account#regenerate-storage-access-keys>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privileged-administrative-users>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-3-manage-application-identities-securely-and-automatically>
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy>
5. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-8-restrict-the-exposure-of-credentials-and-secrets>
6. <https://www.pcidssguide.com/pci-dss-key-rotation-requirements/>
7. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	11.3 <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.			

17.1.2 Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signatures (SAS) can be used to grant limited access to Azure Storage resources. When generating a SAS, it is possible to specify the allowed protocols for a request made with the SAS. It is recommended to allow requests over HTTPS only.

Rationale:

If a SAS is passed over HTTP and intercepted, an attacker performing a man-in-the-middle attack can read the SAS. Then, they can use that SAS just as the intended user could have. This can potentially compromise sensitive data or allow for data corruption by the malicious user.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

It is not possible to audit generated SAS tokens, but Azure Policy can be used to generally audit the existence of configured SAS policy.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [bc1b984e-ddae-40cc-801a-050a030e4fbe](#)
- **Name:** 'Storage accounts should have shared access signature (SAS) policies configured'

Remediation:

Remediate from Azure Portal

If SAS have been created to allow HTTP and were created with a stored access policy (SAP), the SAS can be revoked by deleting the SAP or updating the SAP expiration time to a time in the past:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Containers**, **File shares**, **Queues**, or **Tables**.

4. Click the three dots next to a listed item.
5. Click **Access policy**.
6. Click the three dots next to an access policy.
7. Click **Delete**.
8. Click **Save**.
9. Repeat steps 1-8 as needed to revoke SAS created with SAP.

If SAS have been created to allow HTTP and were not created with a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

When generating a SAS, the default selection for **Allowed protocols** is **HTTPS only**.





References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage>

Additional Information:

This recommendation is based on the recommendation **Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

17.1.3 Ensure that Storage Account Access Keys are Periodically Regenerated (Manual)

Profile Applicability:

- Level 1

Description:

For increased security, regenerate storage account access keys periodically.

Rationale:

When a storage account is created, Azure generates two 512-bit storage access keys which are used for authentication when the storage account is accessed. Rotating these keys periodically ensures that any inadvertent access or exposure does not result from the compromise of these keys.

Cryptographic key rotation periods will vary depending on your organization's security requirements and the type of data which is being stored in the Storage Account. For example, PCI DSS mandates that cryptographic keys be replaced or rotated 'regularly,' and advises that keys for static data stores be rotated every 'few months.'

For the purposes of this recommendation, 90 days will be prescribed for the reminder. Review and adjustment of the 90 day period is recommended, and may even be necessary. Your organization's security requirements should dictate the appropriate setting.

Impact:

Regenerating access keys can affect services in Azure as well as the organization's applications that are dependent on the storage account. All clients who use the access key to access the storage account must be updated to use the new key.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each Storage Account, under **Security + networking**, go to **Access keys**.
3. Review the date and days in the **Last rotated** field for **each** key.

If the **Last rotated** field indicates a number of days greater than 90 [or greater than your organization's period of validity], the key should be rotated.

Audit from Azure CLI

1. Get a list of storage accounts

```
az storage account list --subscription <subscription-id>
```

Make a note of **id**, **name** and **resourceGroup**.

2. For every storage account make sure that key is regenerated in past 90 days.

```
az monitor activity-log list --namespace Microsoft.Storage --offset 90d --  
query "[?contains(authorization.action, 'regenerateKey')]" --resource-id  
<resource id>
```

The output should contain

```
"authorization"/"scope": <your_storage_account> AND "authorization"/"action":  
"Microsoft.Storage/storageAccounts/regeneratekey/action" AND  
"status"/"localizedValue": "Succeeded" "status"/"Value": "Succeeded"
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [044985bb-afe1-42cd-8a36-9d5d42424537](#)
- **Name:** 'Storage account keys should not be expired'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each Storage Account with outdated keys, under **Security + networking**, go to **Access keys**.
3. Click **Rotate key** next to the outdated key, then click **Yes** to the prompt confirming that you want to regenerate the access key.

After Azure regenerates the Access Key, you can confirm that **Access keys** reflects a **Last rotated** date of (**0 days ago**).









Default Value:

By default, access keys are not regenerated periodically.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-create-storage-account#regenerate-storage-access-keys>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privileged-administrative-users>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-2-protect-identity-and-authentication-systems>
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy>
5. <https://www.pcidssguide.com/pci-dss-key-rotation-requirements/>
6. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

17.1.4 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signature (SAS) tokens provide restricted access to Azure Storage resources (such as blobs, files, queues, or tables) for a defined time period with specific permissions. It enables users to interact with the resources without exposing account keys, offering precise control over the permitted actions (e.g., read, write) and the duration of access. To minimize security risks, SAS tokens should be configured with the shortest possible lifespan, ideally lasting no longer than an hour.

Rationale:

A short lifespan for SAS tokens is recommended to minimize the risk of unauthorized access. SAS tokens grant time-limited access to resources, and a longer duration increases the opportunity for misuse if the token is compromised. By setting a shorter lifespan, the potential for security breaches is reduced.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

Currently, SAS token expiration times cannot be audited. Until Microsoft makes the token expiration time a setting rather than a token creation parameter, this recommendation will require manual verification.

Remediation:

Remediate from Azure Portal

If SAS have been created without a short lifespan and were created with a stored access policy (SAP), the SAS can be revoked by deleting the SAP or updating the SAP expiration time to a time in the past:

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data storage**, click **Containers**, **File shares**, **Queues**, or **Tables**.
4. Click the three dots next to a listed item.
5. Click **Access policy**.
6. Click the three dots next to an access policy.
7. Click **Delete**.
8. Click **Save**.

9. Repeat steps 1-8 as needed to revoke SAS created with SAP.

If SAS have been created without a short lifespan and were not created with a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

By default, expiration for shared access signature is set to 8 hours.






References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature>

Additional Information:

This recommendation is based on the recommendation **Ensure that shared access signature (SAS) tokens expire within an hour**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

17.1.5 Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

Every secure request to an Azure Storage account must be authorized. By default, requests can be authorized with either Microsoft Entra credentials or by using the account access key for Shared Key authorization.

Rationale:

Microsoft Entra ID provides superior security and ease of use compared to Shared Key and is recommended by Microsoft. To require clients to use Microsoft Entra ID for authorizing requests, you can disallow requests to the storage account that are authorized with Shared Key.

Impact:

When you disallow Shared Key authorization for a storage account, any requests to the account that are authorized with Shared Key, including shared access signatures (SAS), will be denied. Client applications that currently access the storage account using the Shared Key will no longer function.

Audit:

Audit from Azure Portal

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Settings**, click **Configuration**.
4. Under **Allow storage account key access**, ensure that the radio button next to **Disabled** is selected.
5. Repeat steps 1-4 for each storage account.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

For each storage account, run the following command:

```
az storage account show --resource-group <resource-group> --name <storage-account>
```

Ensure that **allowSharedKeyAccess** is set to **false**.

Audit from PowerShell

Run the following command to list storage accounts:

```
Get-AzStorageAccount
```

Run the following command to get the storage account in a resource group with a given name:

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName <resource-group> -Name <storage-account>
```

Run the following command to get the shared key access setting for the storage account:

```
$storageAccount.allowSharedKeyAccess
```

Ensure that the command returns **False**.
Repeat for each storage account.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [8c6a50c6-9ffd-4ae7-986f-5fa6111f9a54](#)
- **Name:** 'Storage accounts should prevent shared key access'

Remediation:

Remediate from Azure Portal

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Settings**, click **Configuration**.
4. Under **Allow storage account key access**, click the radio button next to **Disabled**.
5. Click **Save**.
6. Repeat steps 1-5 for each storage account requiring remediation.

Remediate from Azure CLI

For each storage account requiring remediation, run the following command to disallow shared key authorization:

```
az storage account update --resource-group <resource-group> --name <storage-account> --allow-shared-key-access false
```

Remediate from PowerShell

For each storage account requiring remediation, run the following command to disallow shared key authorization:


```
Set-AzStorageAccount -ResourceGroupName <resource-group> -Name <storage-  
account> -AllowSharedKeyAccess $false
```












Default Value:

The AllowSharedKeyAccess property of a storage account is not set by default and does not return a value until you explicitly set it. The storage account permits requests that are authorized with the Shared Key when the property value is **null** or when it is **true**.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent>
2. <https://learn.microsoft.com/en-us/cli/azure/storage/account>
3. <https://learn.microsoft.com/en-us/powershell/module/az.storage/get-azstorageaccount>
4. <https://learn.microsoft.com/en-us/powershell/module/az.storage/set-azstorageaccount>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	6.2 <u>Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			
v7	16.7 <u>Establish Process for Revoking Access</u> Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

17.1.6 Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) (Manual)

Profile Applicability:

- Level 2

Description:

Enable sensitive data encryption at rest using Customer Managed Keys (CMK) rather than Microsoft Managed keys.

Rationale:

By default, data in the storage account is encrypted using Microsoft Managed Keys at rest. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted. If you want to control and manage this encryption key yourself, however, you can specify a customer-managed key. That key is used to protect and control access to the key that encrypts your data. You can also choose to automatically update the key version used for Azure Storage encryption whenever a new version is available in the associated Key Vault.

While it is possible to automate the assessment of this recommendation, the assessment status for this recommendation remains 'Manual.' This is because the recommendation pertains to storage accounts that store critical data and is therefore not applicable to all storage accounts.

Impact:

If the key expires by setting the 'activation date' and 'expiration date', the user must rotate the key manually.

Using Customer Managed Keys may also incur additional man-hour requirements to create, store, manage, and protect the keys as needed.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**
2. For each storage account, under **Security + networking**, go to **Encryption**
3. Ensure that **Encryption type** is set to **Customer-managed keys**

Audit from PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription id>
Get-AzStorageAccount |Select-Object -ExpandProperty Encryption
```

PowerShell Results - Non-Compliant

```
...
KeySource                                : Microsoft.Storage
...
```

PowerShell Results - Compliant

```
...
KeySource                                : Microsoft.Keyvault
...
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [6fac406b-40ca-413b-bf8e-0bf964659c25](#)
- **Name:** 'Storage accounts should use customer-managed key for encryption'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**
2. For each storage account, under **Security + networking**, go to **Encryption**
3. Set **Encryption type** to **Customer-managed keys**
4. Select an encryption key or enter a key URI
5. Click **Save**

Default Value:




By default, Encryption type is set to Microsoft Managed Keys.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>
2. <https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-rest>
3. <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption#azure-storage-encryption-versus-disk-encryption>

4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

17.2 Networking

17.2.1 Ensure Private Endpoints are used to access Storage Accounts (Automated)

Profile Applicability:

- Level 2

Description:

Use private endpoints for your Azure Storage accounts to allow clients and services to securely access data located over a network via an encrypted Private Link. To do this, the private endpoint uses an IP address from the VNet for each service. Network traffic between disparate services securely traverses encrypted over the VNet. This VNet can also link addressing space, extending your network and accessing resources on it. Similarly, it can be a tunnel through public networks to connect remote infrastructures together. This creates further security through segmenting network traffic and preventing outside sources from accessing it.

Rationale:

Securing traffic between services through encryption protects the data from easy interception and reading.

Impact:

A Private Endpoint costs approximately US\$7.30 per month. If an Azure Virtual Network is not implemented correctly, this may result in the loss of critical network traffic.

Audit:

Audit from Azure Portal

1. Open the **Storage Accounts** blade.
2. For each listed Storage Account, perform the following check:
3. Under the **Security + networking** heading, click on **Networking**.
4. Click on the **Private endpoint connections** tab at the top of the networking window.
5. Ensure that for each VNet that the Storage Account must be accessed from, a unique Private Endpoint is deployed and the **Connection state** for each Private Endpoint is **Approved**.

Repeat the procedure for each Storage Account.

Audit from PowerShell

```
$storageAccount = Get-AzStorageAccount -ResourceGroup '<ResourceGroupName>' -  
Name '<storageaccountname>'

Get-AzPrivateEndpoint -ResourceGroup '<ResourceGroupName>' | Where-Object  
{$_PrivateLinkServiceConnectionsText -match $storageAccount.id}
```

If the results of the second command returns information, the Storage Account is using a Private Endpoint and complies with this Benchmark, otherwise if the results of the second command are empty, the Storage Account generates a finding.

Audit from Azure CLI

```
az storage account show --name '<storage account name>' --query  
"privateEndpointConnections[0].id"
```

If the above command returns data, the Storage Account complies with this Benchmark, otherwise if the results are empty, the Storage Account generates a finding.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~-/Definitions

- **Policy ID:** [6edd7eda-6dd8-40f7-810d-67160c639cd9](#)
- **Name:** 'Storage accounts should use private link'

Remediation:

Remediate from Azure Portal

1. Open the **Storage Accounts** blade
2. For each listed Storage Account, perform the following:
3. Under the **Security + networking** heading, click on **Networking**
4. Click on the **Private endpoint connections** tab at the top of the networking window
5. Click the **+ Private endpoint** button
6. In the **1 - Basics** tab/step:
 - **Enter a name** that will be easily recognizable as associated with the Storage Account (*Note: The "Network Interface Name" will be automatically completed, but you can customize it if needed.*)
 - Ensure that the **Region** matches the region of the Storage Account
 - Click **Next**
7. In the **2 - Resource** tab/step:
 - Select the **target sub-resource** based on what type of storage resource is being made available
 - Click **Next**
8. In the **3 - Virtual Network** tab/step:
 - Select the **Virtual network** that your Storage Account will be connecting to
 - Select the **Subnet** that your Storage Account will be connecting to
 - (Optional) Select other network settings as appropriate for your environment
 - Click **Next**
9. In the **4 - DNS** tab/step:
 - (Optional) Select other DNS settings as appropriate for your environment
 - Click **Next**
10. In the **5 - Tags** tab/step:
 - (Optional) Set any tags that are relevant to your organization
 - Click **Next**
11. In the **6 - Review + create** tab/step:
 - A validation attempt will be made and after a few moments it should indicate **Validation Passed** - if it does not pass, double-check your settings before beginning more in depth troubleshooting.
 - If validation has passed, click **Create** then wait for a few minutes for the scripted deployment to complete.

Repeat the above procedure for each Private Endpoint required within every Storage Account.

Remediate from PowerShell

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName
'<ResourceGroupName>' -Name '<storageaccountname>'

$privateEndpointConnection = @{
    Name = 'connectionName'
    PrivateLinkServiceId = $storageAccount.Id
    GroupID =
"blob|blob_secondary|file|file_secondary|table|table_secondary|queue|queue_se
condary|web|web_secondary|dfs|dfs_secondary"
}

$privateLinkServiceConnection = New-AzPrivateLinkServiceConnection
@privateEndpointConnection

$virtualNetDetails = Get-AzVirtualNetwork -ResourceGroupName
'<ResourceGroupName>' -Name '<name>'

$privateEndpoint = @{
    ResourceGroupName = '<ResourceGroupName>'
    Name = '<PrivateEndpointName>'
    Location = '<location>'
    Subnet = $virtualNetDetails.Subnets[0]
    PrivateLinkServiceConnection =
$privateLinkServiceConnection
}

New-AzPrivateEndpoint @privateEndpoint
```

Remediate from Azure CLI

```
az network private-endpoint create --resource-group <ResourceGroupName> --
location <location> --name <private endpoint name> --vnet-name <VNET Name> --
subnet <subnet name> --private-connection-resource-id <storage account ID> --
connection-name <private link service connection name> --group-id
<blob|blob_secondary|file|file_secondary|table|table_secondary|queue|queue_se
condary|web|web_secondary|dfs|dfs_secondary>
```

Default Value:

By default, Private Endpoints are not created for Storage Accounts.

References:





1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>
2. <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>
3. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal>

4. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-cli?tabs=dynamic-ip>
5. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-powershell?tabs=dynamic-ip>
6. <https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal>
7. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

Additional Information:

A NAT gateway is the recommended solution for outbound internet access.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	14.1 <u>Segment the Network Based on Sensitivity</u> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			

17.2.2 Ensure that 'Public Network Access' is 'Disabled' for storage accounts (Automated)

Profile Applicability:

- Level 1

Description:

Disallowing public network access for a storage account overrides the public access settings for individual containers in that storage account for Azure Resource Manager Deployment Model storage accounts. Azure Storage accounts that use the classic deployment model will be retired on August 31, 2024.

Rationale:

The default network configuration for a storage account permits a user with appropriate permissions to configure public network access to containers and blobs in a storage account. Keep in mind that public access to a container is always turned off by default and must be explicitly configured to permit anonymous requests. It grants read-only access to these resources without sharing the account key, and without requiring a shared access signature. It is recommended not to provide public network access to storage accounts until, and unless, it is strongly desired. A shared access signature token or Azure AD RBAC should be used for providing controlled and timed access to blob containers.

Impact:

Access will have to be managed using shared access signatures or via Azure AD RBAC.

For classic storage accounts (to be retired on August 31, 2024), each container in the account must be configured to block anonymous access. Either configure all containers or to configure at the storage account level, migrate to the Azure Resource Manager deployment model.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under the **Security + networking** section, click **Networking**.
3. Ensure the **Public network access** setting is set to **Disabled**.

Audit from Azure CLI

Ensure `publicNetworkAccess` is **Disabled**

```
az storage account show --name <storage-account> --resource-group <resource-group> --query "{publicNetworkAccess:publicNetworkAccess}"
```

Audit from PowerShell

For each Storage Account, ensure **PublicNetworkAccess** is **Disabled**

```
Get-AzStorageAccount -Name <storage account name> -ResourceGroupName <resource group name> |select PublicNetworkAccess
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [b2982f36-99f2-4db5-8eff-283140c09693](#)
- **Name:** 'Storage accounts should disable public network access'

Remediation:

Remediate from Azure Portal

First, follow Microsoft documentation and create shared access signature tokens for your blob containers. Then,

1. Go to **Storage Accounts**.
2. For each storage account, under the **Security + networking** section, click **Networking**.
3. Set **Public network access** to **Disabled**.
4. Click **Save**.

Remediate from Azure CLI

Set 'Public Network Access' to **Disabled** on the storage account

```
az storage account update --name <storage-account> --resource-group <resource-group> --public-network-access Disabled
```

Remediate from PowerShell

For each Storage Account, run the following to set the **PublicNetworkAccess** setting to **Disabled**

```
Set-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage account name> -PublicNetworkAccess Disabled
```

Default Value:

By default, **Public Network Access** is set to **Enabled from all networks** for the Storage Account.







References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-manage-access-to-resources>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentation-separation-of-duties-strategy>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>
4. <https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access>
5. <https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal>

Additional Information:

This recommendation is based on the Common Reference Recommendation **Ensure public network access is Disabled**, from the **Common Reference Recommendations > Networking > Virtual Networks (VNETs)** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

17.2.3 Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated)

Profile Applicability:

- Level 1

Description:

Restricting default network access helps to provide a new layer of security, since storage accounts accept connections from clients on any network. To limit access to selected networks, the default action must be changed.

Rationale:

Storage accounts should be configured to deny access to traffic from all networks (including internet traffic). Access can be granted to traffic from specific Azure Virtual networks, allowing a secure network boundary for specific applications to be built. Access can also be granted to public internet IP address ranges to enable connections from specific internet or on-premises clients. When network rules are configured, only applications from allowed networks can access a storage account. When calling from an allowed network, applications continue to require proper authorization (a valid access key or SAS token) to access the storage account.

Impact:

All allowed networks will need to be whitelisted on each specific network, creating administrative overhead. This may result in loss of network connectivity, so do not turn on for critical resources during business hours.

Audit:

Audit from Azure Portal

1. Go to Storage Accounts.
2. For each storage account, under **Security + networking**, click **Networking**.
3. Click the **Firewalls and virtual networks** heading.
4. Ensure that **Public network access** is not set to **Enabled from all networks**.

Audit from Azure CLI

Ensure **defaultAction** is not set to **Allow**.

```
az storage account list --query '[*].networkRuleSet'
```

Audit from PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription ID>
Get-AzStorageAccountNetworkRuleset -ResourceGroupName <resource group> -Name
<storage account name> |Select-Object DefaultAction
```

PowerShell Result - Non-Compliant

```
DefaultAction      : Allow
```

PowerShell Result - Compliant

```
DefaultAction      : Deny
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [34c877ad-507e-4c82-993e-3452a6e0ad3c](#) - **Name:** 'Storage accounts should restrict network access'
- **Policy ID:** [2a1a9cdf-e04d-429a-8416-3bfb72a1b26f](#) - **Name:** 'Storage accounts should restrict network access using virtual network rules'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Security + networking**, click **Networking**.
3. Click the **Firewalls and virtual networks** heading.
4. Set **Public network access** to **Enabled from selected virtual networks and IP addresses**.
5. Add rules to allow traffic from specific networks and IP addresses.
6. Click **Save**.

Remediate from Azure CLI

Use the below command to update **default-action** to **Deny**.

```
az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --default-action Deny
```

Default Value:

By default, Storage Accounts will accept connections from clients on any network.

References:




1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

Additional Information:

This recommendation is based on the Common Reference Recommendation **Ensure Network Access Rules are set to Deny-by-default**, from the **Common Reference Recommendations > Networking > Virtual Networks (VNETs)** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			

17.3 Identity and Access Management

17.4 Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1

Description:

Enable data encryption in transit.

Rationale:

The secure transfer option enhances the security of a storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access storage accounts, the connection must use HTTPS. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. Because Azure storage doesn't support HTTPS for custom domain names, this option is not applied when using a custom domain name.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Settings**, click **Configuration**.
3. Ensure that **Secure transfer required** is set to **Enabled**.

Audit from Azure CLI

Use the below command to ensure the **Secure transfer required** is enabled for all the **Storage Accounts** by ensuring the output contains **true** for each of the **Storage Accounts**.

```
az storage account list --query "[*].[name,enableHttpsTrafficOnly]"
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [404c3081-a854-4457-ae30-26a93ef643f9](#) - **Name:** 'Secure transfer to storage accounts should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Settings**, click **Configuration**.
3. Set **Secure transfer required** to **Enabled**.
4. Click **Save**.

Remediate from Azure CLI

Use the below command to enable **Secure transfer required** for a **Storage Account**

```
az storage account update --name <storageAccountName> --resource-group <resourceGroupName> --https-only true
```





Default Value:

By default, **Secure transfer required** is set to **Disabled**.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations#encryption-in-transit>
2. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_list
3. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_update
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

17.5 Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled' (Automated)

Profile Applicability:

- Level 2

Description:

Enabling encryption at the hardware level on top of the default software encryption for Storage Accounts accessing Azure storage solutions.

Rationale:

Azure Storage automatically encrypts all data in a storage account at the network level using 256-bit AES encryption, which is one of the strongest, FIPS 140-2-compliant block ciphers available. Customers who require higher levels of assurance that their data is secure can also enable 256-bit AES encryption at the Azure Storage infrastructure level for double encryption. Double encryption of Azure Storage data protects against a scenario where one of the encryption algorithms or keys may be compromised. Similarly, data is encrypted even before network transmission and in all backups. In this scenario, the additional layer of encryption continues to protect your data. For the most secure implementation of key based encryption, it is recommended to use a Customer Managed asymmetric RSA 2048 Key in Azure Key Vault.

Impact:

The read and write speeds to the storage will be impacted if both default encryption and Infrastructure Encryption are checked, as a secondary form of encryption requires more resource overhead for the cryptography of information. This performance impact should be considered in an analysis for justifying use of the feature in your environment. Customer-managed keys are recommended for the most secure implementation, leading to overhead of key management. The key will also need to be backed up in a secure location, as loss of the key will mean loss of the information in the storage.

Audit:

Audit from Azure Portal

1. From Azure Portal select the portal menu in the top left.
2. Select **Storage Accounts**.
3. Click on each storage account within each resource group you wish to audit.
4. In the overview, under Security, ensure **Infrastructure encryption** is set to **Enabled**.

Audit from Azure CLI

```
az storage blob show \  
  --account-name <storage-account> \  
  --container-name <container> \  
  --name <blob> \  
  --query "properties.serverEncrypted"
```

Audit from PowerShell

```
$account = Get-AzStorageAccount -ResourceGroupName <resource-group> \  
  -Name <storage-account>  
$blob = Get-AzStorageBlob -Context $account.Context \  
  -Container <container> \  
  -Blob <blob>  
$blob.ICloudBlob.Properties.IsServerEncrypted
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [4733ea7b-a883-42fe-8cac-97454c2a9e4a](#) - **Name:** 'Storage accounts should have infrastructure encryption'

Remediation:

Remediate from Azure Portal

1. During Storage Account creation, in the **Encryption** tab, check the box next to **Enable infrastructure encryption**.

Remediate from Azure CLI

Replace the information within <> with appropriate values:

```
az storage account create \  
  --name <storage-account> \  
  --resource-group <resource-group> \  
  --location <location> \  
  --sku Standard_RAGRS \  
  --kind StorageV2 \  
  --require-infrastructure-encryption
```

Remediate from PowerShell

Replace the information within <> with appropriate values:

```
New-AzStorageAccount -ResourceGroupName <resource_group> \  
  -AccountName <storage-account> \  
  -Location <location> \  
  -SkuName "Standard_RAGRS" \  
  -Kind StorageV2 \  
  -RequireInfrastructureEncryption
```

Enabling Infrastructure Encryption after Storage Account Creation

If infrastructure encryption was not enabled on blob storage creation, there is no **official** way to enable it. Please see the additional information section.

Default Value:

By default, Infrastructure Encryption is disabled in blob creation.




References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-encryption-status>
2. <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>
3. <https://docs.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable>
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default>

Additional Information:

The default service side encryption for Azure Storage is enabled on every block blob, append blob, or page blob that was written to Azure Storage after October 20, 2017. Hardware encryption, however, cannot be enabled on a blob storage after its creation. There are ways to copy all data from a blob storage into another or download and reupload into another blob storage. This could result in data loss and is not recommended.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

17.6 Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated)

Profile Applicability:

- Level 2

Description:

NOTE: This recommendation assumes that the **Public network access** parameter is set to **Enabled from selected virtual networks and IP addresses**. Please ensure the prerequisite recommendation has been implemented before proceeding:

- Ensure Default Network Access Rule for Storage Accounts is Set to Deny

Some Azure services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Azure services to bypass the network rules. These services will then use strong authentication to access the storage account. If the **Allow Azure services on the trusted services list to access this storage account** exception is enabled, the following services are granted access to the storage account: Azure Backup, Azure Data Box, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure File Sync, Azure HDInsight, Azure Import/Export, Azure Monitor, Azure Networking Services, and Azure Site Recovery (when registered in the subscription).

Rationale:

Turning on firewall rules for a storage account will block access to incoming requests for data, including from other Azure services. We can re-enable this functionality by allowing access to **trusted Azure services** through networking exceptions.

Impact:

This creates authentication credentials for services that need access to storage resources so that services will no longer need to communicate via network request. There may be a temporary loss of communication as you set each Storage Account. It is recommended to not do this on mission-critical resources during business hours.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Security + networking**, click **Networking**.
3. Click on the **Firewalls and virtual networks** heading.

4. Under **Exceptions**, ensure that **Allow Azure services on the trusted services list to access this storage account** is checked.

Audit from Azure CLI

Ensure **bypass** contains **AzureServices**

```
az storage account list --query '[*].networkRuleSet'
```

Audit from PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription ID>
Get-AzStorageAccountNetworkRuleset -ResourceGroupName <resource group> -Name
<storage account name> |Select-Object Bypass
```

If the response from the above command is **None**, the storage account configuration is out of compliance with this check. If the response is **AzureServices**, the storage account configuration is in compliance with this check.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [c9d007d0-c057-4772-b18c-01e546713bcd](#) - **Name:** 'Storage accounts should allow access from trusted Microsoft services'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Security + networking**, click **Networking**.
3. Click on the **Firewalls and virtual networks** heading.
4. Under **Exceptions**, check the box next to **Allow Azure services on the trusted services list to access this storage account**.
5. Click **Save**.

Remediate from Azure CLI

Use the below command to update **bypass** to **Azure services**.

```
az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --bypass AzureServices
```

Default Value:







By default, Storage Accounts will accept connections from clients on any network.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	13.5 <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.			
v7	13.3 <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			

17.7 Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)

Profile Applicability:

- Level 1

Description:

The Azure Storage blobs contain data like ePHI or Financial, which can be secret or personal. Data that is erroneously modified or deleted by an application or other storage account user will cause data loss or unavailability.

It is recommended that both Azure Containers with attached Blob Storage and standalone containers with Blob Storage be made recoverable by enabling the **soft delete** configuration. This is to save and recover data when blobs or blob snapshots are deleted.

Rationale:

Containers and Blob Storage data can be incorrectly deleted. An attacker/malicious user may do this deliberately in order to cause disruption. Deleting an Azure Storage blob causes immediate data loss. Enabling this configuration for Azure storage ensures that even if blobs/data were deleted from the storage account, Blobs/data objects are recoverable for a particular time which is set in the "Retention policies," ranging from 7 days to 365 days.

Impact:

Additional storage costs may be incurred as snapshots are retained.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each Storage Account, under **Data management**, go to **Data protection**.
3. Ensure that **Enable soft delete for blobs** is checked.
4. Ensure that **Enable soft delete for containers** is checked.
5. Ensure that the retention period for both is a sufficient length for your organization.

Audit from Azure CLI

Blob Storage: Ensure that the output of the below command contains enabled status as true and days is not empty or null

```
az storage blob service-properties delete-policy show
  --account-name <storageAccount>
  --account-key <accountkey>
```

Azure Containers: Ensure that within **containerDeleteRetentionPolicy**, the **enabled** property is set to **true**.

```
az storage account blob-service-properties show
  --account-name <storageAccount>
  --resource-group <resourceGroup>
```

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each Storage Account, under **Data management**, go to **Data protection**.
3. Check the box next to **Enable soft delete for blobs**.
4. Check the box next to **Enable soft delete for containers**.
5. Set the retention period for both to a sufficient length for your organization.
6. Click **Save**.

Remediate from Azure CLI

Update blob storage retention days in below command

```
az storage blob service-properties delete-policy update --days-retained
<RetentionDaysValue> --account-name <StorageAccountName> --account-key
<AccountKey> --enable true
```

Update container retention with the below command

```
az storage account blob-service-properties update
  --enable-container-delete-retention true
  --container-delete-retention-days <days>
  --account-name <storageAccount>
  --resource-group <resourceGroup>
```

Default Value:







Soft delete for containers and blob storage is **enabled** by default on storage accounts created via the Azure Portal, and **disabled** by default on storage accounts created via Azure CLI or PowerShell.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-soft-delete>
2. <https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-container-overview>

3. <https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-container-enable?tabs=azure-portal>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 <u>Establish and Maintain a Data Recovery Process</u> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10.4 <u>Ensure Protection of Backups</u> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

17.8 Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated)

Profile Applicability:

- Level 2

Description:

The Storage Queue service stores messages that may be read by any client who has access to the storage account. A queue can contain an unlimited number of messages, each of which can be up to 64KB in size using version 2011-08-18 or newer. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the queues. Storage Logging log entries contain the following information about individual requests: Timing information such as start time, end-to-end latency, and server latency, authentication details, concurrency information, and the sizes of the request and response messages.

Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

Impact:

Enabling this setting can have a high impact on the cost of the log analytics service and data storage used by logging more data per each request. Do not enable this without determining your need for this level of logging, and do not forget to check in on data usage and projected cost. Some users have seen their logging costs increase from \$10 per month to \$10,000 per month.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Monitoring**, click **Diagnostics settings**.
3. Select the **queue** tab indented below the storage account.
4. Ensure that at least one diagnostic setting is listed.
5. Click **Edit setting** on a diagnostic setting.
6. Ensure that at least one diagnostic setting has **StorageRead**, **StorageWrite**, and **StorageDelete** options selected under the **Logs** section and that they are sent to an appropriate destination.

Audit from Azure CLI

Ensure the below command's output contains properties **delete**, **read** and **write** set to **true**.

```
az storage logging show --services q --account-name <storageAccountName>
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [7bd000e3-37c7-4928-9f31-86c4b77c5c45](#) - **Name:** 'Configure diagnostic settings for Queue Services to Log Analytics workspace'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Monitoring**, click **Diagnostics settings**.
3. Select the **queue** tab indented below the storage account.
4. To create a new diagnostic setting, click **+ Add diagnostic setting**. To update an existing diagnostic setting, click **Edit setting** on the diagnostic setting.
5. Check the boxes next to **StorageRead**, **StorageWrite**, and **StorageDelete**.
6. Select an appropriate destination.
7. Click **Save**.

Remediate from Azure CLI

Use the below command to enable the Storage Logging for Queue service.

```
az storage logging update --account-name <storageAccountName> --account-key <storageAccountKey> --services q --log rwd --retention 90
```

Default Value:

By default storage account queue services are not logged.





References:

1. <https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging>
2. <https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-4-enable-network-logging-for-security-investigation>
4. <https://docs.microsoft.com/en-us/azure/storage/queues/monitor-queue-storage?tabs=azure-portal>

Additional Information:

We cannot practically generalize detailed audit log requirements for every queue due to their nature and intent. This recommendation may be applicable to storage account queue services where the security is paramount.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.9 Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated)

Profile Applicability:

- Level 2

Description:

The Storage Blob service provides scalable, cost-efficient object storage in the cloud. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the blobs. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.

Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor each individual request to a storage service for increased security or diagnostics. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

Impact:

Being a level 2, enabling this setting can have a high impact on the cost of data storage used for logging more data per each request. Do not enable this without determining your need for this level of logging or forget to check in on data usage and projected cost.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Monitoring**, click **Diagnostics settings**.
3. Select the **blob** tab indented below the storage account.
4. Ensure that at least one diagnostic setting is listed.
5. Click **Edit setting** on a diagnostic setting.
6. Ensure that at least one diagnostic setting has **StorageRead**, **StorageWrite**, and **StorageDelete** options selected under the **Logs** section and that they are sent to an appropriate destination.

Audit from Azure CLI

Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services b --account-name <storageAccountName>
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [b4fe1a3b-0715-4c6c-a5ea-ffc33cf823cb](#) - **Name:** 'Configure diagnostic settings for Blob Services to Log Analytics workspace'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Monitoring**, click **Diagnostics settings**.
3. Select the **blob** tab indented below the storage account.
4. To create a new diagnostic setting, click **+ Add diagnostic setting**. To update an existing diagnostic setting, click **Edit setting** on the diagnostic setting.
5. Check the boxes next to **StorageRead**, **StorageWrite**, and **StorageDelete**.
6. Select an appropriate destination.
7. Click **Save**.

Remediate from Azure CLI

Use the below command to enable the Storage Logging for Blob service.

```
az storage logging update --account-name <storageAccountName> --account-key <storageAccountKey> --services b --log rwd --retention 90
```

Default Value:

By default, storage account blob service logging is disabled for read, write, and delete operations.





References:

1. <https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging>
2. <https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection/#lt-3-enable-logging-for-security-investigation>

Additional Information:

We cannot practically generalize detailed audit log requirements for every blob due to their nature and intent. This recommendation may be applicable to storage account blob service where the security is paramount.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.10 Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated)

Profile Applicability:

- Level 2

Description:

Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schema-less design. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the tables. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.

Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor each individual request to a storage service for increased security or diagnostics. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

Impact:

Being a level 2, enabling this setting can have a high impact on the cost of data storage used for logging more data per each request. Do not enable this without determining your need for this level of logging or forget to check in on data usage and projected cost.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Monitoring**, click **Diagnostics settings**.
3. Select the **table** tab indented below the storage account.
4. Ensure that at least one diagnostic setting is listed.
5. Click **Edit setting** on a diagnostic setting.
6. Ensure that at least one diagnostic setting has **StorageRead**, **StorageWrite**, and **StorageDelete** options selected under the **Logs** section and that they are sent to an appropriate destination.

Audit from Azure CLI

Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services t --account-name <storageAccountName>
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [2fb86bf3-d221-43d1-96d1-2434af34eaa0](#) - **Name:** 'Configure diagnostic settings for Table Services to Log Analytics workspace'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Monitoring**, click **Diagnostics settings**.
3. Select the **table** tab indented below the storage account.
4. To create a new diagnostic setting, click **+ Add diagnostic setting**. To update an existing diagnostic setting, click **Edit setting** on the diagnostic setting.
5. Check the boxes next to **StorageRead**, **StorageWrite**, and **StorageDelete**.
6. Select an appropriate destination.
7. Click **Save**.

Remediate from Azure CLI

Use the below command to enable the Storage Logging for Table service.

```
az storage logging update --account-name <storageAccountName> --account-key <storageAccountKey> --services t --log rwd --retention 90
```

Default Value:

By default, storage account table service logging is disabled for read, write, and delete operations





References:

1. <https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging>
2. <https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

Additional Information:

We cannot practically generalize detailed audit log requirements for every table due to their nature and intent. This recommendation may be applicable to storage account table service where the security is paramount.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

17.11 Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2' (Automated)

Profile Applicability:

- Level 1

Description:

In some cases, Azure Storage sets the minimum TLS version to be version 1.0 by default. TLS 1.0 is a legacy version and has known vulnerabilities. This minimum TLS version can be configured to be later protocols such as TLS 1.2.

Rationale:

TLS 1.0 has known vulnerabilities and has been replaced by later versions of the TLS protocol. Continued use of this legacy protocol affects the security of data in transit.

Impact:

When set to TLS 1.2 all requests must leverage this version of the protocol. Applications leveraging legacy versions of the protocol will fail.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Settings**, click **Configuration**.
3. Ensure that the **Minimum TLS version** is set to **Version 1.2**.

Audit from Azure CLI

Get a list of all storage accounts and their resource groups

```
az storage account list | jq '.[ ] | {name, resourceGroup}'
```

Then query the minimumTLSVersion field

```
az storage account show \
  --name <storage-account> \
  --resource-group <resource-group> \
  --query minimumTlsVersion \
  --output tsv
```

Audit from PowerShell

To get the minimum TLS version, run the following command:

```
(Get-AzStorageAccount -Name <STORAGEACCOUNTNAME> -ResourceGroupName  
<RESOURCEGROUPNAME>).MinimumTlsVersion
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [fe83a0eb-a853-422d-aac2-1bffd182c5d0](#) - **Name:** 'Storage accounts should have the specified minimum TLS version'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Settings**, click **Configuration**.
3. Set the **Minimum TLS version** to **Version 1.2**.
4. Click **Save**.

Remediate from Azure CLI

```
az storage account update \  
  --name <storage-account> \  
  --resource-group <resource-group> \  
  --min-tls-version TLS1_2
```

Remediate from PowerShell

To set the minimum TLS version, run the following command:

```
Set-AzStorageAccount -AccountName <STORAGEACCOUNTNAME> \  
  -ResourceGroupName <RESOURCEGROUPNAME> \  
  -MinimumTlsVersion TLS1_2
```

Default Value:





If a storage account is created through the portal, the MinimumTlsVersion property for that storage account will be set to TLS 1.2.

If a storage account is created through PowerShell or CLI, the MinimumTlsVersion property for that storage account will not be set, and defaults to TLS 1.0.

References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/transport-layer-security-configure-minimum-version?tabs=portal>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

17.12 Ensure 'Cross Tenant Replication' is not enabled (Automated)

Profile Applicability:

- Level 1

Description:

Cross Tenant Replication in Azure allows data to be replicated across multiple Azure tenants. While this feature can be beneficial for data sharing and availability, it also poses a significant security risk if not properly managed. Unauthorized data access, data leakage, and compliance violations are potential risks. Disabling Cross Tenant Replication ensures that data is not inadvertently replicated across different tenant boundaries without explicit authorization.

Rationale:

Disabling Cross Tenant Replication minimizes the risk of unauthorized data access and ensures that data governance policies are strictly adhered to. This control is especially critical for organizations with stringent data security and privacy requirements, as it prevents the accidental sharing of sensitive information.

Impact:

Disabling Cross Tenant Replication may affect data availability and sharing across different Azure tenants. Ensure that this change aligns with your organizational data sharing and availability requirements.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Data management**, click **Object replication**.
3. Click **Advanced settings**.
4. Ensure **Allow cross-tenant replication** is not checked.

Audit from Azure CLI

```
az storage account list --query "[*].[name,allowCrossTenantReplication]"
```

The value of **false** should be returned for each storage account listed.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [92a89a79-6c52-4a7e-a03f-61306fc49312](#) - **Name:** 'Storage accounts should prevent cross tenant object replication'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Data management**, click **Object replication**.
3. Click **Advanced settings**.
4. Uncheck **Allow cross-tenant replication**.
5. Click **OK**.

Remediate from Azure CLI

Replace the information within <> with appropriate values:

```
az storage account update --name <storageAccountName> --resource-group  
<resourceGroupName> --allow-cross-tenant-replication false
```






Default Value:

For new storage accounts created after Dec 15, 2023 cross tenant replication is not enabled.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-prevent-cross-tenant-policies?tabs=portal>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	13.4 <u>Only Allow Access to Authorized Cloud Storage or Email Providers</u> Only allow access to authorized cloud storage or email providers.			

17.13 Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

The Azure Storage setting 'Allow Blob Anonymous Access' (aka "allowBlobPublicAccess") controls whether anonymous access is allowed for blob data in a storage account. When this property is set to True, it enables public read access to blob data, which can be convenient for sharing data but may carry security risks. When set to False, it disallows public access to blob data, providing a more secure storage environment.

Rationale:

If "Allow Blob Anonymous Access" is enabled, blobs can be accessed by adding the blob name to the URL to see the contents. An attacker can enumerate a blob using methods, such as brute force, and access them.

Exfiltration of data by brute force enumeration of items from a storage account may occur if this setting is set to 'Enabled'.

Impact:

Additional consideration may be required for exceptional circumstances where elements of a storage account require public accessibility. In these circumstances, it is highly recommended that all data stored in the public facing storage account be reviewed for sensitive or potentially compromising data, and that sensitive or compromising data is never stored in these storage accounts.

Audit:

Audit from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Settings**, click **Configuration**.
3. Ensure **Allow Blob Anonymous Access** is set to **Disabled**.

Audit from Azure CLI

For every storage account in scope:

```
az storage account show --name "<yourStorageAccountName>" --query allowBlobPublicAccess
```

Ensure that every storage account in scope returns **false** for the "allowBlobPublicAccess" setting.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [4fa4b6c0-31ca-4c0d-b10d-24b96f62a751](#) - **Name:** '[Preview]: Storage account public access should be disallowed'

Remediation:

Remediate from Azure Portal

1. Go to **Storage Accounts**.
2. For each storage account, under **Settings**, click **Configuration**.
3. Set **Allow Blob Anonymous Access** to **Disabled**.
4. Click **Save**.

Remediate from Powershell

For every storage account in scope, run the following:

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName  
"<yourResourceGroup>" -Name "<yourStorageAccountName>"  
$storageAccount.AllowBlobPublicAccess = $false  
Set-AzStorageAccount -InputObject $storageAccount
```

Default Value:

Disabled







References:

1. <https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent?tabs=portal>
2. <https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent?source=recommendations&tabs=portal>
3. Classic Storage Accounts: <https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent-classic?tabs=portal>

Additional Information:

Azure Storage accounts that use the classic deployment model will be retired on August 31, 2024.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

17.14 Ensure Azure Resource Manager Delete locks are applied to Azure Storage Accounts (Manual)

Profile Applicability:

- Level 1

Description:

Azure Resource Manager *CannotDelete* (*Delete*) locks can prevent users from accidentally or maliciously deleting a storage account. This feature ensures that while the Storage account can still be modified or used, deletion of the Storage account resource requires removal of the lock by a user with appropriate permissions.

This feature is a protective control for the availability of data. By ensuring that a storage account or its parent resource group cannot be deleted without first removing the lock, the risk of data loss is reduced.

Rationale:

Applying a *Delete* lock on storage accounts protects the availability of data by preventing the accidental or unauthorized deletion of the entire storage account. It is a fundamental protective control that can prevent data loss

Impact:

- Prevents the deletion of the Storage account Resource entirely.
- Prevents the deletion of the parent Resource Group containing the locked Storage account resource.
- Does not prevent other control plane operations, including modification of configurations, network settings, containers, and access.
- Does not prevent deletion of containers or other objects within the storage account.

Audit:

Audit from Azure Portal

1. Navigate to the storage account in the Azure portal.
2. For each storage account, under **Settings**, click **Locks**.
3. Ensure that a **Delete** lock exists on the storage account.

Audit from Azure CLI

```
az lock list --resource-group <resource-group> \
             --resource-name <storage-account> \
             --resource-type "Microsoft.Storage/storageAccounts"
```

Audit from PowerShell

```
Get-AzResourceLock -ResourceGroupName <RESOURCEGROUPNAME> `
                  -ResourceName <STORAGEACCOUNTNAME> `
                  -ResourceType "Microsoft.Storage/storageAccounts"
```

Audit from Azure Policy

There is currently no built-in Microsoft policy to audit resource locks on storage accounts.

Custom and community policy definitions can check for the existence of a “Microsoft.Authorization/locks” resource with an AuditIfNotExists effect.

Remediation:

Remediate from Azure Portal

1. Navigate to the storage account in the Azure portal.
2. Under the **Settings** section, select **Locks**.
3. Select **Add**.
4. Provide a Name, and choose **Delete** for the type of lock.
5. Add a note about the lock if desired.

Remediate from Azure CLI

Replace the information within <> with appropriate values:

```
az lock create --name <lock> \
               --resource-group <resource-group> \
               --resource <storage-account> \
               --lock-type CanNotDelete \
               --resource-type Microsoft.Storage/storageAccounts
```

Remediate from PowerShell

Replace the information within <> with appropriate values:

```
New-AzResourceLock -LockLevel CanNotDelete `
                  -LockName <lock> `
                  -ResourceName <storage-account> `
                  -ResourceType Microsoft.Storage/storageAccounts `
                  -ResourceGroupName <resource-group>
```

Default Value:

By default, no locks are applied to Azure resources, including storage accounts. Locks must be manually configured after resource creation.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/lock-account-resource>
2. <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3 <u>Data Protection</u> Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.			

17.15 Ensure Azure Resource Manager ReadOnly locks are considered for Azure Storage Accounts (Manual)

Profile Applicability:

- Level 2

Description:

Adding an Azure Resource Manager **ReadOnly** lock can prevent users from accidentally or maliciously deleting a storage account, modifying its properties and containers, or creating access assignments. The lock must be removed before the storage account can be deleted or updated. It provides more protection than a **CannotDelete**-type of resource manager lock.

This feature prevents **POST** operations on a storage account and containers to the Azure Resource Manager control plane, *management.azure.com*. Blocked operations include **listKeys** which prevents clients from obtaining the account shared access keys.

Microsoft does not recommend **ReadOnly** locks for storage accounts with Azure Files and Table service containers.

This Azure Resource Manager REST API documentation (spec) provides information about the control plane **POST** operations for *Microsoft.Storage* resources.

Rationale:

Applying a **ReadOnly** lock on storage accounts protects the confidentiality and availability of data by preventing the accidental or unauthorized deletion of the entire storage account and modification of the account, container properties, or access permissions. It can offer enhanced protection for blob and queue workloads with tradeoffs in usability and compatibility for clients using account shared access keys.

Impact:

- Prevents the deletion of the Storage account Resource entirely.
- Prevents the deletion of the parent Resource Group containing the locked Storage account resource.
- Prevents clients from obtaining the storage account shared access keys using a **listKeys** operation.
- Requires Entra credentials to access blob and queue data in the Portal.
- Data in Azure Files or the Table service may be inaccessible to clients using the account shared access keys.
- Prevents modification of account properties, network settings, containers, and RBAC assignments.
- Does not prevent access using existing account shared access keys issued to clients.

- Does not prevent deletion of containers or other objects within the storage account.

Audit:

Audit from Azure Portal

1. Navigate to the storage account in the Azure portal.
2. For each storage account, under **Settings**, click **Locks**.
3. Ensure that a **ReadOnly** lock exists on the storage account.

Audit from Azure CLI

```
az lock list --resource-group <resource-group> \
            --resource-name <storage-account> \
            --resource-type "Microsoft.Storage/storageAccounts"
```

Audit from PowerShell

```
Get-AzResourceLock -ResourceGroupName <RESOURCEGROUPNAME> `
                  -ResourceName <STORAGEACCOUNTNAME> `
                  -ResourceType "Microsoft.Storage/storageAccounts"
```

Audit from Azure Policy

There is currently no built-in Microsoft policy to audit resource locks on storage accounts.

Custom and community policy definitions can check for the existence of a “Microsoft.Authorization/locks” resource with an AuditIfNotExists effect.

Remediation:

Remediate from Azure Portal

1. Navigate to the storage account in the Azure portal.
2. Under the **Settings** section, select **Locks**.
3. Select **Add**.
4. Provide a Name, and choose **ReadOnly** for the type of lock.
5. Add a note about the lock if desired.

Remediate from Azure CLI

Replace the information within <> with appropriate values:

```
az lock create --name <lock> \
              --resource-group <resource-group> \
              --resource <storage-account> \
              --lock-type ReadOnly \
              --resource-type Microsoft.Storage/storageAccounts
```

Remediate from PowerShell

Replace the information within <> with appropriate values:

```
New-AzResourceLock -LockLevel ReadOnly `
                    -LockName <lock> `
                    -ResourceName <storage-account> `
                    -ResourceType Microsoft.Storage/storageAccounts `
                    -ResourceGroupName <resource-group>
```

Default Value:

By default, no locks are applied to Azure resources, including storage accounts. Locks must be manually configured after resource creation.

References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/lock-account-resource>
2. <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>
3. <https://github.com/Azure/azure-rest-api-specs/tree/main/specification/storage>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3 Data Protection Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.			

17.16 Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts (Automated)

Profile Applicability:

- Level 2

Description:

Geo-redundant storage (GRS) in Azure replicates data three times within the primary region using locally redundant storage (LRS) and asynchronously copies it to a secondary region hundreds of miles away. This setup ensures high availability and resilience by providing 16 nines (99.99999999999999%) durability over a year, safeguarding data against regional outages.

Rationale:

Enabling GRS protects critical data from regional failures by maintaining a copy in a geographically separate location. This significantly reduces the risk of data loss, supports business continuity, and meets high availability requirements for disaster recovery.

Impact:

Enabling geo-redundant storage on Azure storage accounts increases costs due to cross-region data replication.

Audit:

Audit from Azure Portal

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data management**, click **Redundancy**.
4. Ensure that **Redundancy** is set to **Geo-redundant storage (GRS)**.
5. Repeat steps 1-4 for each storage account.

Audit from Azure CLI

Run the following command to list storage accounts:

```
az storage account list
```

For each storage account, run the following command:

```
az storage account show --resource-group <resource-group> --name <storage-account>
```

Under **sku**, ensure that **name** is set to **Standard_GRS**.

Audit from PowerShell

Run the following command to list storage accounts:

```
Get-AzStorageAccount
```

Run the following command to get the storage account in a resource group with a given name:

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName <resource-group> -Name <storage-account>
```

Run the following command to get the redundancy setting for the storage account:

```
$storageAccount.SKU.Name
```

Ensure that the command returns **Standard_GRS**.

Repeat for each storage account.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [bf045164-79ba-4215-8f95-f8048dc1780b](#)
- **Name:** 'Geo-redundant storage should be enabled for Storage Accounts'

Remediation:

Remediate from Azure Portal

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Data management**, click **Redundancy**.
4. From the **Redundancy** drop-down menu, select **Geo-redundant storage (GRS)**.
5. Click **Save**.
6. Repeat steps 1-5 for each storage account requiring remediation.

Remediate from Azure CLI

For each storage account requiring remediation, run the following command to enable geo-redundant storage:

```
az storage account update --resource-group <resource-group> --name <storage-account> --sku Standard_GRS
```

Remediate from PowerShell

For each storage account requiring remediation, run the following command to enable geo-redundant storage:

```
Set-AzStorageAccount -ResourceGroupName <resource-group> -Name <storage-account> -SkuName "Standard_GRS"
```

Default Value:

When creating a storage account in the Azure Portal, the default redundancy setting is geo-redundant storage (GRS). Using the Azure CLI, the default is read-access geo-redundant storage (RA-GRS). In PowerShell, a redundancy level must be explicitly specified during account creation.

References:




1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy>
2. <https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration>
3. <https://learn.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az-storage-account-update>
4. <https://learn.microsoft.com/en-us/powershell/module/az.storage/set-azstorageaccount?view=azps-12.4.0>
5. <https://learn.microsoft.com/en-us/azure/storage/common/storage-disaster-recovery-guidance>

Additional Information:

When choosing the best redundancy option, weigh the trade-offs between lower costs and higher availability. Key factors to consider include:

- The method of data replication within the primary region.
- The replication of data from a primary to a geographically distant secondary region for protection against regional disasters (geo-replication).
- The necessity for read access to replicated data in the secondary region during an outage in the primary region (geo-replication with read access).

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 <u>Establish and Maintain a Data Recovery Process</u> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	10 <u>Data Recovery Capabilities</u> Data Recovery Capabilities			

18 Storage Explorer

This section covers security best practice recommendations for Storage Explorer.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:

<https://workbench.cisecurity.org/communities/72>.

Resources for Storage Explorer

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/storage/storage-explorer/>

Storage Explorer service overview:

- <https://learn.microsoft.com/en-us/azure/storage/storage-explorer/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows>

Microsoft Cloud Security Baseline for Storage:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline>

18.1 Ensure that shared access signature (SAS) tokens expire within an hour (Manual)

Profile Applicability:

- Level 1

Description:

Shared access signature (SAS) tokens provide restricted access to Azure Storage resources (such as blobs, files, queues, or tables) for a defined time period with specific permissions. It enables users to interact with the resources without exposing account keys, offering precise control over the permitted actions (e.g., read, write) and the duration of access. To minimize security risks, SAS tokens should be configured with the shortest possible lifespan, ideally lasting no longer than an hour.

Rationale:

A short lifespan for SAS tokens is recommended to minimize the risk of unauthorized access. SAS tokens grant time-limited access to resources, and a longer duration increases the opportunity for misuse if the token is compromised. By setting a shorter lifespan, the potential for security breaches is reduced.

Impact:

SAS can pose security risks if they are not managed carefully.

Audit:

Currently, SAS token expiration times cannot be audited. Until Microsoft makes the token expiration time a setting rather than a token creation parameter, this recommendation will require manual verification.

Remediation:

Remediate from Storage Explorer

If SAS have been created without a short lifespan and were created with a stored access policy (SAP), the SAS can be revoked by deleting the SAP or updating the SAP expiration time to a time in the past:

1. In Storage Explorer, expand **Storage Accounts**.
2. Expand a storage account.
3. Expand **Blob Containers**, **File Shares**, **Queues**, or **Tables**, and right-click a blob container, file share, queue, or table.
4. Click **Manage Stored Access Policies....**
5. Click the trash icon next to a stored access policy.
6. Click **Save**.
7. Repeat steps 1-6 as needed to revoke SAS created with SAP.

Remediate from Azure Portal

If SAS have been created without a short lifespan and were not created with a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

By default, expiration for shared access signature created from Storage Explorer is set to 24 hours.






References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
2. <https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature>
3. <https://learn.microsoft.com/en-us/azure/storage/storage-explorer/vs-azure-tools-storage-explorer-blobs#manage-access-policies-for-a-blob-container>

Additional Information:

This recommendation is based on the recommendation **Ensure that shared access signature (SAS) tokens expire within an hour**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 <u>Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16.7 <u>Establish Process for Revoking Access</u> Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.			

18.2 Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)

Profile Applicability:

- Level 1

Description:

Use stored access policies (SAP) when generating shared access signature (SAS) tokens in Azure to centrally manage permissions, expiration, and revocation settings for resource access. Stored access policies can be applied to blob containers, file shares, queues, and tables.

Rationale:

Stored access policies provide centralized control over SAS token access, allowing administrators to update permissions or revoke access. This approach strengthens security by reducing the risk of unauthorized access to storage resources.

Impact:

There is no cost for creating stored access policies, however there is some administrative overhead involved in managing these policies.

Audit:

It is not currently possible to retrieve a list of all generated SAS tokens to check if they were associated with a SAP during creation.

An SAS token that has been created with a SAP will contain an **si** parameter that references the stored access policy identifier associated with the SAS, e.g.

si=<stored-access-policy-identifier>.

The **si** parameter will be absent from an SAS token created without a SAP.

Remediation:

Remediate from Storage Explorer

To create a SAP:

1. In Storage Explorer, expand **Storage Accounts**.
2. Expand a storage account.
3. Expand **Blob Containers**, **File Shares**, **Queues**, or **Tables**, and right-click a blob container, file share, queue, or table.
4. Click **Manage Stored Access Policies....**
5. Under **Access Policies**, click **Add**.
6. Modify the **ID**, **Start time**, **Expiry time**, and permissions appropriately.
7. Click **Save**.
8. Repeat steps 1-7 as needed to create SAP.

When generating SAS, select a SAP from the **Access policy** drop-down.

Remediate from Azure Portal

If SAS have been created without a SAP, the SAS can be revoked by regenerating the storage account access keys:

Note: Regenerating access keys can affect any applications or Azure services that are dependent on the storage account key.

1. Go to **Storage accounts**.
2. Click on a storage account.
3. Under **Security + networking**, click **Access keys**.
4. Next to each key, click **Rotate key**.
5. Click **Yes** to confirm.
6. Repeat steps 1-5 as needed to revoke SAS.

Default Value:

By default, stored access policies are not associated with SAS. To use a stored access policy, it must be explicitly created and linked to the SAS at the time of creation.







References:

1. <https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview#best-practices-when-using-sas>
2. <https://learn.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy>
3. <https://learn.microsoft.com/en-us/azure/storage/storage-explorer/vs-azure-tools-storage-explorer-blobs#manage-access-policies-for-a-blob-container>

Additional Information:

This recommendation is based on the recommendation **Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens**, from the **Common Reference Recommendations > Secrets and Keys > Shared Access Signatures** section.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.2 Establish an Access Revoking Process</u> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<u>14.6 Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

18.3 Ensure Storage Explorer is using the latest version (Manual)

Profile Applicability:

- Level 1

Description:

Ensure all users accessing Azure Storage resources with Storage Explorer are using the latest version of the software, applying updates promptly to safeguard against new vulnerabilities and benefit from the latest security enhancements.

Rationale:

Using the latest version of Storage Explorer is essential for safeguarding access to Azure Storage resources.

Impact:

Using the latest version of Storage Explorer is free and requires minimal administrative effort.

Audit:

Audit from Storage Explorer for MacOS

1. Go to **Storage Explorer**.
2. From the menu bar, click **Microsoft Azure Storage Explorer**.
3. Click **About**.
4. Check the **Version** listed.
5. Compare the installed version with the latest released version from <https://github.com/microsoft/AzureStorageExplorer/releases>.
6. Ensure that the installed Storage Explorer version matches the latest released version.

Remediation:

Remediate from Storage Explorer for MacOS

1. Go to **Storage Explorer**.
2. From the menu bar, click **Microsoft Azure Storage Explorer**.
3. Click **Check for Updates**.
4. Follow the instructions to install the latest version of Storage Explorer.







Default Value:

By default, new installations of Storage Explorer will utilize the latest released version.

References:

1. <https://azure.microsoft.com/en-us/products/storage/storage-explorer/#Overview>
2. <https://github.com/microsoft/AzureStorageExplorer/releases>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

19 Azure Container Storage

No specific prescriptive guidance exists yet for Azure Container Storage.

Help us improve this Benchmark! If you notice a needed correction, want to provide feedback, or wish to contribute security best practice guidance please join our community and create a ticket, propose a change, or start a discussion so we can improve this guidance!

The CIS Microsoft Azure Community is here:

<https://workbench.cisecurity.org/communities/72>.

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Resources for Azure Container Storage

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/container-storage/>

Azure Container Storage service overview:

- <https://learn.microsoft.com/en-us/azure/storage/container-storage/container-storage-introduction>

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Introduction		
1.1	CIS Microsoft Azure Foundations Benchmarks		
1.2	CIS Microsoft Azure Service Category Benchmarks		
1.3	Multiple Methods of Audit and Remediation		
2	Common Reference Recommendations		
2.1	Secrets and Keys		
2.1.1	Shared Access Signatures		
2.1.1.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Encryption Key Management		
2.1.2.1	Microsoft Managed Keys		
2.1.2.1.1	Ensure Critical Data is Encrypted with Microsoft Managed Keys (MMK) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.2	Customer Managed Keys		
2.1.2.2.1	Ensure Critical Data is Encrypted with Customer Managed Keys (CMK) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.3	Customer Provided Keys		
2.2	Networking		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.1	Virtual Networks (VNETs)		
2.2.1.1	Ensure public network access is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure Network Access Rules are set to Deny-by-default (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Private Endpoints		
2.2.2.1	Ensure Private Endpoints are used to access {service} (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Private Link		
2.3	Identity and Access Management		
2.4	Logging		
3	Archive Storage (Reference)		
4	Azure Managed Lustre		
4.1	Ensure 'Key encryption key' is set to a customer-managed key for Azure Managed Lustre file systems (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5	Azure Backup		
5.1	Backup Vaults		
5.1.1	Ensure soft delete on Backup vaults is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure immutability for Backup vaults is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Backup vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.5	Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Recovery Services Vaults		
5.2.1	Ensure soft delete on Recovery Services vaults is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure immutability for Recovery Services vaults is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure backup data in Recovery Services vaults is encrypted using customer-managed keys (CMK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Recovery Services vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure public network access on Recovery Services vaults is Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6	Azure Data Lake Storage (Reference)		
7	Azure Data Share		
8	Azure Files		
8.1	Ensure soft delete for Azure File Shares is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure root squash for NFS file shares is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.3	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.4	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9	Azure Storage Actions (Preview)		
10	Azure NetApp Files		
10.1	Ensure 'Encryption key source' is set to 'Customer Managed Key' for Azure NetApp Files accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
11	Azure Blob Storage		
11.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
11.2	Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
11.3	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
11.4	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
11.5	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
11.6	Ensure locked immutability policies are used for containers storing business-critical blob data (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
12	Azure Data Box		
12.1	Ensure double encryption is used for Azure Data Box in high-security environments (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
13	Azure Disk Storage (Reference)		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
14	Azure Confidential Ledger		
15	Azure Elastic SAN		
15.1	Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure customer-managed keys (CMK) are used to encrypt data at rest on Azure Elastic SAN volume groups (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
16	Queue Storage		
16.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
16.2	Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
16.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17	Storage Accounts		
17.1	Secrets and Keys		
17.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17.1.2	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17.1.3	Ensure that Storage Account Access Keys are Periodically Regenerated (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17.1.4	Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17.1.5	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.1.6	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17.2	Networking		
17.2.1	Ensure Private Endpoints are used to access Storage Accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.2.3	Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.3	Identity and Access Management		
17.4	Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.5	Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.6	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.7	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.8	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.9	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.10	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.11	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
17.12	Ensure 'Cross Tenant Replication' is not enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.13	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
17.14	Ensure Azure Resource Manager Delete locks are applied to Azure Storage Accounts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17.15	Ensure Azure Resource Manager ReadOnly locks are considered for Azure Storage Accounts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
17.16	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
18	Storage Explorer		
18.1	Ensure that shared access signature (SAS) tokens expire within an hour (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
18.2	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
18.3	Ensure Storage Explorer is using the latest version (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
19	Azure Container Storage		

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure public network access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure soft delete on Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure immutability for Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure soft delete on Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure immutability for Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure public network access on Recovery Services vaults is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure soft delete for Azure File Shares is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure root squash for NFS file shares is configured	<input type="checkbox"/>	<input type="checkbox"/>
11.3	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
11.4	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
11.5	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.6	Ensure locked immutability policies are used for containers storing business-critical blob data	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
15.1	Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN	<input type="checkbox"/>	<input type="checkbox"/>
16.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
17.1.5	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.7	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	<input type="checkbox"/>	<input type="checkbox"/>
17.13	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
18.2	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
18.3	Ensure Storage Explorer is using the latest version	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure public network access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2.1	Ensure Private Endpoints are used to access {service}	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure soft delete on Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure immutability for Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure soft delete on Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure immutability for Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure public network access on Recovery Services vaults is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure soft delete for Azure File Shares is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure root squash for NFS file shares is configured	<input type="checkbox"/>	<input type="checkbox"/>
8.3	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>
8.4	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
11.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
11.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
11.3	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
11.4	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
11.5	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.6	Ensure locked immutability policies are used for containers storing business-critical blob data	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN	<input type="checkbox"/>	<input type="checkbox"/>
16.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
16.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
16.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
17.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	<input type="checkbox"/>	<input type="checkbox"/>
17.1.2	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
17.1.3	Ensure that Storage Account Access Keys are Periodically Regenerated	<input type="checkbox"/>	<input type="checkbox"/>
17.1.4	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
17.1.5	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.2.1	Ensure Private Endpoints are used to access Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.4	Ensure that 'Secure transfer required' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
17.7	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	<input type="checkbox"/>	<input type="checkbox"/>
17.8	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>
17.9	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>
17.10	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	<input type="checkbox"/>	<input type="checkbox"/>
17.11	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	<input type="checkbox"/>	<input type="checkbox"/>
17.12	Ensure 'Cross Tenant Replication' is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
17.13	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
18.1	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
18.2	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
18.3	Ensure Storage Explorer is using the latest version	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.1.1	Ensure Critical Data is Encrypted with Microsoft Managed Keys (MMK)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.2.1	Ensure Critical Data is Encrypted with Customer Managed Keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure public network access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure Network Access Rules are set to Deny-by-default	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2.1	Ensure Private Endpoints are used to access {service}	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure 'Key encryption key' is set to a customer-managed key for Azure Managed Lustre file systems	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure soft delete on Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure immutability for Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure soft delete on Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure immutability for Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.2.3	Ensure backup data in Recovery Services vaults is encrypted using customer-managed keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure public network access on Recovery Services vaults is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure soft delete for Azure File Shares is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure root squash for NFS file shares is configured	<input type="checkbox"/>	<input type="checkbox"/>
8.3	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>
8.4	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>
10.1	Ensure 'Encryption key source' is set to 'Customer Managed Key' for Azure NetApp Files accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
11.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
11.3	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
11.4	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
11.5	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.6	Ensure locked immutability policies are used for containers storing business-critical blob data	<input type="checkbox"/>	<input type="checkbox"/>
12.1	Ensure double encryption is used for Azure Data Box in high-security environments	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure customer-managed keys (CMK) are used to encrypt data at rest on Azure Elastic SAN volume groups	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
16.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
16.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
16.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
17.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	<input type="checkbox"/>	<input type="checkbox"/>
17.1.2	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
17.1.3	Ensure that Storage Account Access Keys are Periodically Regenerated	<input type="checkbox"/>	<input type="checkbox"/>
17.1.4	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
17.1.5	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.1.6	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
17.2.1	Ensure Private Endpoints are used to access Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.2.3	Ensure Default Network Access Rule for Storage Accounts is Set to Deny	<input type="checkbox"/>	<input type="checkbox"/>
17.4	Ensure that 'Secure transfer required' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.5	Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.6	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	<input type="checkbox"/>	<input type="checkbox"/>
17.7	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	<input type="checkbox"/>	<input type="checkbox"/>
17.8	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>
17.9	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
17.10	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	<input type="checkbox"/>	<input type="checkbox"/>
17.11	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	<input type="checkbox"/>	<input type="checkbox"/>
17.12	Ensure 'Cross Tenant Replication' is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
17.13	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
18.1	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
18.2	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
18.3	Ensure Storage Explorer is using the latest version	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
17.14	Ensure Azure Resource Manager Delete locks are applied to Azure Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.15	Ensure Azure Resource Manager ReadOnly locks are considered for Azure Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure public network access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure soft delete on Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure immutability for Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure soft delete on Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure immutability for Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure public network access on Recovery Services vaults is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure soft delete for Azure File Shares is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure root squash for NFS file shares is configured	<input type="checkbox"/>	<input type="checkbox"/>
11.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
11.3	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
11.4	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
11.5	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN	<input type="checkbox"/>	<input type="checkbox"/>
16.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
16.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
17.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	<input type="checkbox"/>	<input type="checkbox"/>
17.1.3	Ensure that Storage Account Access Keys are Periodically Regenerated	<input type="checkbox"/>	<input type="checkbox"/>
17.1.4	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
17.1.5	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.6	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	<input type="checkbox"/>	<input type="checkbox"/>
17.7	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	<input type="checkbox"/>	<input type="checkbox"/>
17.12	Ensure 'Cross Tenant Replication' is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
17.13	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.16	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
18.1	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
18.2	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
18.3	Ensure Storage Explorer is using the latest version	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.1.1	Ensure Critical Data is Encrypted with Microsoft Managed Keys (MMK)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.2.1	Ensure Critical Data is Encrypted with Customer Managed Keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure public network access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure Network Access Rules are set to Deny-by-default	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2.1	Ensure Private Endpoints are used to access {service}	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure 'Key encryption key' is set to a customer-managed key for Azure Managed Lustre file systems	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure soft delete on Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure immutability for Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure soft delete on Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure immutability for Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.2.3	Ensure backup data in Recovery Services vaults is encrypted using customer-managed keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure public network access on Recovery Services vaults is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure soft delete for Azure File Shares is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure root squash for NFS file shares is configured	<input type="checkbox"/>	<input type="checkbox"/>
8.3	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>
8.4	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>
10.1	Ensure 'Encryption key source' is set to 'Customer Managed Key' for Azure NetApp Files accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
11.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
11.3	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
11.4	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
11.5	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.6	Ensure locked immutability policies are used for containers storing business-critical blob data	<input type="checkbox"/>	<input type="checkbox"/>
12.1	Ensure double encryption is used for Azure Data Box in high-security environments	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure customer-managed keys (CMK) are used to encrypt data at rest on Azure Elastic SAN volume groups	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
16.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
16.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
16.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
17.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	<input type="checkbox"/>	<input type="checkbox"/>
17.1.2	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
17.1.3	Ensure that Storage Account Access Keys are Periodically Regenerated	<input type="checkbox"/>	<input type="checkbox"/>
17.1.4	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
17.1.5	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.1.6	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
17.2.1	Ensure Private Endpoints are used to access Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.2.3	Ensure Default Network Access Rule for Storage Accounts is Set to Deny	<input type="checkbox"/>	<input type="checkbox"/>
17.4	Ensure that 'Secure transfer required' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.5	Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.6	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	<input type="checkbox"/>	<input type="checkbox"/>
17.7	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	<input type="checkbox"/>	<input type="checkbox"/>
17.8	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>
17.9	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
17.10	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	<input type="checkbox"/>	<input type="checkbox"/>
17.11	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	<input type="checkbox"/>	<input type="checkbox"/>
17.12	Ensure 'Cross Tenant Replication' is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
17.13	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.16	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
18.1	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
18.2	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
18.3	Ensure Storage Explorer is using the latest version	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.1.1	Ensure Critical Data is Encrypted with Microsoft Managed Keys (MMK)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2.2.1	Ensure Critical Data is Encrypted with Customer Managed Keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.1	Ensure public network access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1.2	Ensure Network Access Rules are set to Deny-by-default	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2.1	Ensure Private Endpoints are used to access {service}	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure 'Key encryption key' is set to a customer-managed key for Azure Managed Lustre file systems	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure soft delete on Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure immutability for Backup vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure soft delete on Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure immutability for Recovery Services vaults is Enabled	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.2.3	Ensure backup data in Recovery Services vaults is encrypted using customer-managed keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure 'Use infrastructure encryption for this vault' is enabled on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	Ensure public network access on Recovery Services vaults is Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults	<input type="checkbox"/>	<input type="checkbox"/>
8.1	Ensure soft delete for Azure File Shares is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure root squash for NFS file shares is configured	<input type="checkbox"/>	<input type="checkbox"/>
8.3	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>
8.4	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	<input type="checkbox"/>	<input type="checkbox"/>
10.1	Ensure 'Encryption key source' is set to 'Customer Managed Key' for Azure NetApp Files accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
11.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
11.3	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	<input type="checkbox"/>	<input type="checkbox"/>
11.4	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
11.5	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
11.6	Ensure locked immutability policies are used for containers storing business-critical blob data	<input type="checkbox"/>	<input type="checkbox"/>
12.1	Ensure double encryption is used for Azure Data Box in high-security environments	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure customer-managed keys (CMK) are used to encrypt data at rest on Azure Elastic SAN volume groups	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
16.1	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
16.2	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
16.3	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
17.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	<input type="checkbox"/>	<input type="checkbox"/>
17.1.2	Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only'	<input type="checkbox"/>	<input type="checkbox"/>
17.1.3	Ensure that Storage Account Access Keys are Periodically Regenerated	<input type="checkbox"/>	<input type="checkbox"/>
17.1.4	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
17.1.5	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.1.6	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
17.2.1	Ensure Private Endpoints are used to access Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	<input type="checkbox"/>	<input type="checkbox"/>
17.2.3	Ensure Default Network Access Rule for Storage Accounts is Set to Deny	<input type="checkbox"/>	<input type="checkbox"/>
17.4	Ensure that 'Secure transfer required' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.5	Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.6	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	<input type="checkbox"/>	<input type="checkbox"/>
17.7	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	<input type="checkbox"/>	<input type="checkbox"/>
17.8	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>
17.9	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
17.10	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	<input type="checkbox"/>	<input type="checkbox"/>
17.11	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	<input type="checkbox"/>	<input type="checkbox"/>
17.12	Ensure 'Cross Tenant Replication' is not enabled	<input type="checkbox"/>	<input type="checkbox"/>
17.13	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
17.16	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts	<input type="checkbox"/>	<input type="checkbox"/>
18.1	Ensure that shared access signature (SAS) tokens expire within an hour	<input type="checkbox"/>	<input type="checkbox"/>
18.2	Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens	<input type="checkbox"/>	<input type="checkbox"/>
18.3	Ensure Storage Explorer is using the latest version	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Oct 28, 2024	1.0.0	ADDED - Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled' (Ticket 22883)
Nov 12, 2024	1.0.0	ADDED - Ensure that shared access signature (SAS) tokens expire within an hour (Ticket 22879)
Nov 12, 2024	1.0.0	ADDED - Ensure Azure Resource Manager ReadOnly locks are considered for Azure Storage Accounts (Ticket 22963)
Nov 12, 2024	1.0.0	ADDED - Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts (Ticket 22931)
Nov 12, 2024	1.0.0	ADDED - Storage Explorer - Ensure that shared access signature (SAS) tokens have a short lifespan (Ticket 23040)
Nov 12, 2024	1.0.0	ADDED - Storage Explorer - Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Ticket 23047)
Nov 13, 2024	1.0.0	ADDED - Azure Blob Storage - Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Ticket 22973)
Nov 13, 2024	1.0.0	ADDED - Azure Blob Storage - Ensure that shared access signature (SAS) tokens expire within an hour (Ticket 23038)
Nov 13, 2024	1.0.0	ADDED - Azure Blob Storage - Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled (Ticket 22779)
Nov 13, 2024	1.0.0	ADDED - Azure Blob Storage - Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Ticket 23042)
Nov 13, 2024	1.0.0	ADDED - Azure Blob Storage - Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts (Ticket 23036)

Date	Version	Changes for this version
Nov 13, 2024	1.0.0	ADDED - Azure Blob Storage - Ensure locked immutability policies are used for containers storing business-critical blob data (Ticket 23050)
Nov 13, 2024	1.0.0	ADDED - Azure Data Box - Ensure double encryption is used for Azure Data Box in high-security environments (Ticket 22950)
Nov 13, 2024	1.0.0	ADDED - Azure NetApp Files - Ensure 'Encryption key source' is set to 'Customer Managed Key' for Azure NetApp Files accounts (Ticket 23002)
Nov 13, 2024	1.0.0	ADDED - Azure Files - Ensure soft delete for Azure File Shares is Enabled (Ticket 22829)
Nov 13, 2024	1.0.0	ADDED - Azure Files - Ensure root squash for NFS file shares is configured (Ticket 22928)
Nov 13, 2024	1.0.0	ADDED - Azure Files - Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares (Ticket 22990)
Nov 13, 2024	1.0.0	ADDED - Azure Files - Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares (Ticket 22993)
Nov 13, 2024	1.0.0	ADDED - Backup Vaults - Ensure soft delete on Backup vaults is Enabled (Ticket 22847)
Nov 13, 2024	1.0.0	ADDED - Backup Vaults - Ensure immutability for Backup vaults is Enabled (Ticket 22849)
Nov 13, 2024	1.0.0	ADDED - Backup Vaults - Ensure backup data in Backup vaults is encrypted using customer-managed keys (CMK) (Ticket 22891)
Nov 13, 2024	1.0.0	ADDED - Backup Vaults - Ensure 'Use infrastructure encryption for this vault' is enabled on Backup vaults (Ticket 22980)
Nov 13, 2024	1.0.0	ADDED - Backup Vaults - Ensure 'Cross Region Restore' is set to 'Enabled' on Backup vaults (Ticket 23009)

Date	Version	Changes for this version
Nov 13, 2024	1.0.0	ADDED - Backup Vaults - Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Backup vaults (Ticket 23031)
Nov 13, 2024	1.0.0	ADDED - Recovery Services Vaults - Ensure soft delete on Recovery Services vaults is Enabled (Ticket 22848)
Nov 13, 2024	1.0.0	ADDED - Recovery Services Vaults - Ensure immutability for Recovery Services vaults is Enabled (Ticket 22850)
Nov 13, 2024	1.0.0	ADDED - Recovery Services Vaults - Ensure backup data in Recovery Services vaults is encrypted using customer-managed keys (CMK) (Ticket 22906)
Nov 13, 2024	1.0.0	ADDED - Recovery Services Vaults - Ensure 'Use infrastructure encryption for this vault' is enabled on Recovery Services vaults (Ticket 22960)
Nov 13, 2024	1.0.0	ADDED - Recovery Services Vaults - Ensure public network access on Recovery Services vaults is Disabled (Ticket 22835)
Nov 13, 2024	1.0.0	ADDED - Recovery Services Vaults - Ensure 'Cross Region Restore' is set to 'Enabled' on Recovery Services vaults (Ticket 23016)
Nov 13, 2024	1.0.0	ADDED - Recovery Services Vaults - Ensure 'Cross Subscription Restore' is set to 'Disabled' or 'Permanently Disabled' on Recovery Services vaults (Ticket 23034)
Nov 13, 2024	1.0.0	ADDED - Azure Managed Lustre - Ensure 'Key encryption key' is set to a customer-managed key for Azure Managed Lustre file systems (Ticket 22988)
Nov 13, 2024	1.0.0	ADDED - Azure Elastic SAN - Ensure 'Public network access' is set to 'Disabled' on Azure Elastic SAN (Ticket 22889)
Nov 13, 2024	1.0.0	ADDED - Azure Elastic SAN - Ensure customer-managed keys (CMK) are used to encrypt data at rest on Azure Elastic SAN volume groups (Ticket 22940)
Nov 13, 2024	1.0.0	ADDED - Queue Storage - Ensure 'Allowed Protocols' for shared access signature (SAS) tokens is set to 'HTTPS Only' (Ticket 22786)

Date	Version	Changes for this version
Nov 13, 2024	1.0.0	ADDED - Queue Storage - Ensure that shared access signature (SAS) tokens expire within an hour (Ticket 23039)
Nov 13, 2024	1.0.0	ADDED - Queue Storage - Ensure stored access policies (SAP) are used when generating shared access signature (SAS) tokens (Ticket 23046)
Nov 13, 2024	1.0.0	ADDED - Storage Explorer - Ensure Storage Explorer is using the latest version (Ticket 23041)