CIS Microsoft Azure Foundations Benchmark

v4.0.0 - 03-23-2025

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 (legalnotices@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

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 completes 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 document, CIS Microsoft Azure Foundations Benchmark, provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure. This Benchmark is scoped to establish foundational security for tenancy in the Microsoft Azure cloud services platform. For Cloud Service Providers, the "Foundations" Benchmark is meant to be used as a first step which is complimented by "Service Category" Benchmarks as a second step. This relationship is further explained in the "Introduction" section. Section overviews are used extensively in this document to provide specific and very important context - review section overviews diligently.

The sections of this document are titled to reflect the product category names found in the Microsoft Azure Product Directory. These categorical sections are then divided into subsections that will be titled to reflect the specific services being addressed. Recommendations will be found in these subsections if "Foundational" recommendations are available for the service, OR if a Service Category Benchmark has not yet been created to address the Service Category.

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
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	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
Mike Wicks
Zeeshan Mustafa
Jim Cheng
Gareth Boyes
Zan Liffick
Iben Rodriguez
Sagar Chhatrala
Jeffrey Lemmermann
Richard Rives
Nirbhay Kumar
Michael Born
Bhushan Bhat
Harshal Khachane
Karan Ahuja
RAHUL PAREEK
Luke Schultheis
Ben Habing
Andrei Stefanie
Rajaniesh Kaushikk

Editor
Rachel Rice
Steve Johnson
Robert Burton
Niclas Madsen
Ian McRee

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. Previous releases may 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 Foundations 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 provides an object-based method of evaluating configuration states and other governance detail. Information for the purpose of automating Azure Policy evaluation can be found in the "Automating using Azure Policy" section below.

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/installation?view=graph-powershell-1.0

DEPRECATION WARNING: Starting March 30, 2025, MSOnline (MSOL), and AzureAD cmdlet modules will no longer be supported and are scheduled for full retirement within 6 months. If you have used these cmdlet modules for any scripting or automation, you should immediately review and update potentially affected materials. For additional detail, review this blog post from Microsoft: https://techcommunity.microsoft.com/blog/microsoft-entra-blog/action-required-msonline-and-azuread-powershell-retirement---2025-info-and-resou/4364991

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
```

If you receive a message indicating `InteractiveBrowserCredential authentication failed`, disable web account manager (WAM) to force a browser authentication with the following command:

```
Update-AzConfig -EnableLoginByWam $false
```

Then attempt using 'Connect-AzAccount' again.

If the browser-based login is not available, you may need to use device-code authentication, but this should be avoided and is not recommended because it is a persistent authentication method and specifically blocked by recommendations found in the Azure Benchmarks. Instructions for this method will not be provided as it is not recommended.

For the Graph PowerShell module, the log in method is the same.

```
Connect-MgGraph
```

Automating using Azure Policy

Azure Policy provides built-in objects that can be used to evaluate and/or enforce configuration states for individual resources or groups of resources. Where a relevant Azure Policy object or multiple Policy objects have been identified as applicable to a recommendation in this Benchmark, the Policy ID(s) and associated Policy Name will be listed in the "From Azure Policy" method header.

Policy evaluation scans can be launched or reviewed through the Azure Portal, Azure CLI, Azure PowerShell, REST API, or using a GitHub Action. Scoping and filtering an Azure Policy evaluation is necessary to ensure that the query is relevant to the architecture and requirements of an organization. Azure Policy evaluation can be batched together and structured using a "Compliance Initiative" or Policy Set which is constructed in a JSON file.

Resources to assist with the use of Azure Policy:

- Retrieving Azure Policy information: https://learn.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data
- Querying Policy States with REST API: https://learn.microsoft.com/en-us/rest/api/policy/policy-states
- Azure Policy GitHub Action: https://github.com/marketplace/actions/azure-policy-compliance-scan
- AzPolicyAdvertizer - database of Azure Policy objects and related material: https://www.azadvertizer.net/azpolicyadvertizer_all.html
- General Azure Policy Documentation: https://learn.microsoft.com/en-us/azure/governance/policy/

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 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.

2.1.1.1 Microsoft Managed Keys

2.1.1.1.1 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 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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1041

2.1.1.2 Customer Managed Keys

2.1.1.2.1 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 wants 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 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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1041

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 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"**

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1037

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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1037

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:

If an Azure Virtual Network is not implemented correctly, this may result in the loss of critical network traffic.

Private endpoints are charged per hour of use. Refer to https://azure.microsoft.com/en-us/pricing/details/private-link/ and https://azure.microsoft.com/en-us/pricing/calculator/ to estimate potential costs.

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.

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

- Storage Services > Storage Accounts > Networking > **"Ensure Private Endpoints are used to access Storage Accounts"**

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	14.1 Segment the Network Based on Sensitivity 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).		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1537	TA0010	M1037

3 Analytics Services

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#analytics

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

3.1 Azure Databricks

3.1.1 Ensure that Azure Databricks is deployed in a customer-managed virtual network (VNet) (Automated)

Profile Applicability:

- Level 1

Description:

Networking for Azure Databricks can be set up in a few different ways. Using a customer-managed Virtual Network (VNet) (also known as VNet Injection) ensures that compute clusters and control planes are securely isolated within the organization's network boundary. By default, Databricks creates a managed VNet, which provides limited control over network security policies, firewall configurations, and routing.

Rationale:

Using a customer-managed VNet ensures better control over network security and aligns with zero-trust architecture principles. It allows for:

- Restricted outbound internet access to prevent unauthorized data exfiltration.
- Integration with on-premises networks via VPN or ExpressRoute for hybrid connectivity.
- Fine-grained NSG policies to restrict access at the subnet level.
- Private Link for secure API access, avoiding public internet exposure.

Impact:

- Requires additional configuration during Databricks workspace deployment.
- Might increase operational overhead for network maintenance.
- May impact connectivity if misconfigured (e.g., restrictive NSG rules or missing routes).

Audit:

Audit from Azure Portal

1. Go to Azure Portal → Search for Databricks Workspaces.
2. Select the Databricks Workspace to audit.
3. Under Networking, check if the workspace is deployed in a Customer-Managed VNet.
4. If the Virtual Network field shows Databricks-Managed VNet, it is non-compliant.
5. Verify NSG rules and Private Endpoints for fine-grained access control.

Audit from Azure CLI
Run the following command to check if Databricks is using a customer-managed VNet:

```
az network vnet show --resource-group <resource-group-name> --name <vnet-
name>
```

Ensure that Databricks subnets are present in the VNet configuration.
Validate NSG rules attached to the Databricks subnets.

Audit from PowerShell

```
Get-AzDatabricksWorkspace -ResourceGroupName <resource-group-name> -Name
<databricks-workspace-name> | Select-Object VirtualNetworkId
```

If VirtualNetworkId is null or shows a Databricks-Managed VNet, it is non-compliant.

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:** 9c25c9e4-ee12-4882-afd2-11fb9d87893f **- Name:** 'Azure Databricks Workspaces should be in a virtual network'

Remediation:

Remediate from Azure Portal

1. Delete the existing Databricks workspace (migration required).
2. Create a new Databricks workspace with VNet Injection:
3. Go to Azure Portal → Create Databricks Workspace.
4. Select Advanced Networking.
5. Choose Deploy into your own Virtual Network.
6. Specify a customer-managed VNet and associated subnets.
7. Enable Private Link for secure API access.

Remediate from Azure CLI
Deploy a new Databricks workspace in a custom VNet:

```
az databricks workspace create --name <databricks-workspace-name> \
    --resource-group <resource-group-name> \
    --location <region> \
    --managed-resource-group <managed-rg-name> \
    --enable-no-public-ip true \
    --network-security-group-rule "NoAzureServices" \
    --public-network-access Disabled \
    --custom-virtual-network-id /subscriptions/<subscription-
id>/resourceGroups/<resource-group-
name>/providers/Microsoft.Network/virtualNetworks/<vnet-name>
```

Ensure NSG Rules are correctly configured:

```
az network nsg rule create --resource-group <resource-group-name> \
    --nsg-name <nsg-name> \
    --name "DenyAllOutbound" \
    --direction Outbound \
    --access Deny \
    --priority 4096
```

Remediate from PowerShell

```
New-AzDatabricksWorkspace -ResourceGroupName <resource-group-name> -Name
<databricks-workspace-name> -Location <region> -ManagedResourceGroupName
<managed-rg-name> -CustomVirtualNetworkId "/subscriptions/<subscription-
id>/resourceGroups/<resource-group-
name>/providers/Microsoft.Network/virtualNetworks/<vnet-name>"
```

Default Value:

By default, Azure Databricks uses a Databricks-Managed VNet.

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	14.1 Segment the Network Based on Sensitivity 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).		●	●

3.1.2 Ensure that network security groups are configured for Databricks subnets (Manual)

Profile Applicability:

- Level 1

Description:

Network Security Groups (NSGs) should be implemented to control inbound and outbound traffic to Azure Databricks subnets, ensuring only authorized communication. NSGs should be configured with deny rules to block unwanted traffic and restrict communication to essential sources only.

Rationale:

Impact:

- NSGs require periodic maintenance to ensure rule accuracy.
- Misconfigured NSGs could inadvertently block required traffic.

Audit:

Audit from Azure Portal

1. Navigate to Virtual Networks > Subnets, and review NSG assignments.

Audit from Azure CLI

```
az network nsg list --query "[].{Name:name, Rules:securityRules}"
```

Audit from PowerShell

```
Get-AzNetworkSecurityGroup -ResourceGroupName <resource-group-name>
```

Remediation:

Remediate from Azure Portal

1. Assign NSG to Databricks subnets under Networking > NSG Settings.

Default Value:

By default, Databricks subnets do not have NSGs assigned.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-databricks-security-baseline

2. https://learn.microsoft.com/en-us/azure/databricks/security/network/classic/vnet-inject#network-security-group-rules

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

3.1.3 Ensure that traffic is encrypted between cluster worker nodes (Manual)

Profile Applicability:

- Level 2

Description:

By default, data exchanged between worker nodes in an Azure Databricks cluster is not encrypted. To ensure that data is encrypted at all times, whether at rest or in transit, you can create an initialization script that configures your clusters to encrypt traffic between worker nodes using AES 256-bit encryption over a TLS 1.3 connection.

Rationale:

- Protects sensitive data during transit between cluster nodes, mitigating risks of data interception or unauthorized access.
- Aligns with organizational security policies and compliance requirements that mandate encryption of data in transit.
- Enhances overall security posture by ensuring that all inter-node communications within the cluster are encrypted.

Impact:

- Enabling encryption may introduce a performance penalty due to the computational overhead associated with encrypting and decrypting traffic. This can result in longer query execution times, especially for data-intensive operations.
- Implementing encryption requires creating and managing init scripts, which adds complexity to cluster configuration and maintenance.
- The shared encryption secret is derived from the hash of the keystore stored in DBFS. If the keystore is updated or rotated, all running clusters must be restarted to prevent authentication failures between Spark workers and drivers.

Audit:

Audit from Azure Portal
Review cluster init scripts:

1. Navigate to your Azure Databricks workspace, go to the "Clusters" section, select a cluster, and check the "Advanced Options" for any init scripts that configure encryption settings.

Verify spark configuration:

2. Ensure that the following Spark configurations are set:

```
spark.authenticate true
spark.authenticate.enableSaslEncryption true
spark.network.crypto.enabled true
spark.network.crypto.keyLength 256
spark.network.crypto.keyFactoryAlgorithm PBKDF2WithHmacSHA1
spark.io.encryption.enabled true
```

These settings can be found in the cluster's Spark configuration properties.
Check keystone management:

3. Verify that the Java KeyStore (JKS) file is securely stored in DBFS and that its integrity is maintained.
4. Ensure that the keystore password is securely managed and not hardcoded in scripts.

Remediation:

Create a JKS keystore:

1. Generate a Java KeyStore (JKS) file that will be used for SSL/TLS encryption.
2. Upload the keystore file to a secure directory in DBFS (e.g. /dbfs//jetty_ssl_driver_keystore.jks).

Develop an init script:

3. Create an init script that performs the following tasks:
    - Retrieves the JKS keystore file and password.
    - Derives a shared encryption secret from the keystore.
    - Configures Spark driver and executor settings to enable encryption.

4. Example init script: *[next page]*

```
#!/bin/bash
set -euo pipefail
keystore_dbfs_file="/dbfs/<keystore-
directory>/jetty_ssl_driver_keystore.jks"
max_attempts=30
while [ ! -f ${keystore_dbfs_file} ]; do
  if [ "$max_attempts" == 0 ]; then
    echo "ERROR: Unable to find the file : $keystore_dbfs_file. Failing
the script."
    exit 1
  fi
  sleep 2s
  ((max_attempts--))
done
sasl_secret=$(sha256sum $keystore_dbfs_file | cut -d' ' -f1)
if [ -z "${sasl_secret}" ]; then
  echo "ERROR: Unable to derive the secret. Failing the script."
  exit 1
fi
local_keystore_file="$DB_HOME/keys/jetty_ssl_driver_keystore.jks"
local_keystore_password="gb1gQqZ9ZIHS"
if [[ $DB_IS_DRIVER = "TRUE" ]]; then
  driver_conf=${DB_HOME}/driver/conf/spark-branch.conf
  echo "Configuring driver conf at $driver_conf"
  if [ ! -e $driver_conf ]; then
    echo "spark.authenticate true" >> $driver_conf
    echo "spark.authenticate.secret $sasl_secret" >> $driver_conf
    echo "spark.authenticate.enableSaslEncryption true" >> $driver_conf
    echo "spark.network.crypto.enabled true" >> $driver_conf
    echo "spark.network.crypto.keyLength 256" >> $driver_conf
    echo "spark.network.crypto.keyFactoryAlgorithm PBKDF2WithHmacSHA1"
>> $driver_conf
    echo "spark.io.encryption.enabled true" >> $driver_conf
    echo "spark.ssl.enabled true" >> $driver_conf
    echo "spark.ssl.keyPassword $local_keystore_password" >>
$driver_conf
    echo "spark.ssl.keyStore $local_keystore_file" >> $driver_conf
    echo "spark.ssl.keyStorePassword $local_keystore_password" >>
$driver_conf
    echo "spark.ssl.protocol TLSv1.3" >> $driver_conf
  fi
fi
executor_conf=${DB_HOME}/conf/spark.executor.extraJavaOptions
echo "Configuring executor conf at $executor_conf"
if [ ! -e $executor_conf ]; then
  echo "-Dspark.authenticate=true" >> $executor_conf
  echo "-Dspark.authenticate.secret=$sasl_secret" >> $executor_conf
  echo "-Dspark.authenticate.enableSaslEncryption=true" >>
$executor_conf
  echo "-Dspark.network.crypto.enabled=true" >> $executor_conf
  echo "-Dspark.network.crypto.keyLength=256" >> $executor_conf
  echo "-Dspark.network.crypto.keyFactoryAlgorithm=PBKDF2WithHmacSHA1"
>> $executor_conf
  echo "-Dspark.io.encryption.enabled=true" >> $executor_conf
  echo "-Dspark.ssl.enabled=true" >> $executor_conf
  echo "-Dspark.ssl.keyPassword=$local_keystore_password" >>
$executor_conf
```

```
  echo "-Dspark.ssl.keyStore=$local_keystore_file" >> $executor_conf
  echo "-Dspark.ssl.keyStorePassword=$local_keystore_password" >>
$executor_conf
  echo "-Dspark.ssl.protocol=TLSv1.3" >> $executor_conf
fi
```

5. Save.

Default Value:

By default, traffic is not encrypted between cluster worker nodes.

References:

1. https://learn.microsoft.com/en-us/azure/databricks/security/keys/encrypt-otw

CIS Controls:

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

3.1.4 Ensure that users and groups are synced from Microsoft Entra ID to Azure Databricks (Manual)

Profile Applicability:

- Level 1

Description:

To ensure centralized identity and access management, users and groups from Microsoft Entra ID should be synchronized with Azure Databricks. This is achieved through SCIM provisioning, which automates the creation, update, and deactivation of users and groups in Databricks based on Entra ID assignments. Enabling this integration ensures that access controls in Databricks remain consistent with corporate identity governance policies, reducing the risk of orphaned accounts, stale permissions, and unauthorized access.

Rationale:

Syncing users and groups from Microsoft Entra ID centralizes access control, enforces the least privilege principle by automatically revoking unnecessary access, reduces administrative overhead by eliminating manual user management, and ensures auditability and compliance with industry regulations.

Impact:

SCIM provisioning requires role mapping to avoid misconfigured user privileges.

Audit:

Audit from Azure Portal
Verify SCIM provisioning is enabled:

1. Go to `Microsoft Entra ID`.
2. Under `Manage`, click `Enterprise applications`.
3. Click the name of the Azure Databricks SCIM application.
4. Under `Provisioning`, confirm that SCIM provisioning is enabled and running.

Check user sync status in Azure Portal:

5. Under `Provisioning Logs`, verify the last successful sync and any failed entries.

Check user sync status in Databricks:

6. Go to `Admin Console` > `Identity and Access Management`.
7. Confirm that Users and Groups match those assigned in Microsoft Entra ID.

Ensure role-based access control (RBAC) mapping is correct:

8. Verify that users are assigned appropriate Databricks roles (e.g. Admin, User, Contributor).
9. Confirm that groups are mapped to workspace access roles.

Remediation:

Remediate from Azure Portal
Enable provisioning in Azure Portal:

1. Go to `Microsoft Entra ID`.
2. Under `Manage`, click `Enterprise applications`.
3. Click the name of the Azure Databricks SCIM application.
4. Under `Provisioning`, select `Automatic` and enter the SCIM endpoint and API token from Databricks.

Enable provisioning in Databricks:

5. Navigate to `Admin Console` > `Identity and Access Management`.
6. Enable SCIM provisioning and generate an API token.

Configure role assignments:

7. Ensure groups from Entra ID are mapped to appropriate Databricks roles.
8. Restrict administrative privileges to designated security groups.

Regularly monitor sync logs:

9. Periodically review sync logs in Microsoft Entra ID and Databricks Admin Console.
10. Configure Azure Monitor alerts for provisioning failures.

Disable manual user creation in Databricks:

11. Ensure that all user management is controlled via SCIM sync from Entra ID.
12. Disable personal access token usage for authentication.

Remediate from Azure CLI
Enable SCIM User and Group Provisioning in Azure Databricks:

```
az ad app update --id <databricks-app-id> --set
provisioning.provisioningMode=Automatic
```

Default Value:

By default, Azure Databricks does not sync users and groups from Microsoft Entra ID.

References:

1. https://learn.microsoft.com/en-us/azure/databricks/administration-guide/users-groups/scim/aad

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

3.1.5 Ensure that Unity Catalog is configured for Azure Databricks (Manual)

Profile Applicability:

- Level 1

Description:

Unity Catalog is a centralized governance model for managing and securing data in Azure Databricks. It provides fine-grained access control to databases, tables, and views using Microsoft Entra ID identities. Unity Catalog also enhances data lineage, audit logging, and compliance monitoring, making it a critical component for security and governance.

Rationale:

- Enforces centralized access control policies and reduces data security risks.
- Enables identity-based authentication via Microsoft Entra ID.
- Improves compliance with industry regulations (e.g. GDPR, HIPAA, SOC 2) by providing audit logs and access visibility.
- Prevents unauthorized data access through table-, row-, and column-level security (RLS & CLS).

Impact:

- Improperly configured permissions may lead to data exfiltration or unauthorized access.
- Unity Catalog requires structured governance policies to be effective and prevent overly permissive access.

Audit:

Method 1: Verify unity catalog deployment:

1. As an Azure Databricks account admin, log into the account console.
2. Click Workspaces.
3. Find your workspace and check the Metastore column. If a metastore name is present, your workspace is attached to a Unity Catalog metastore and therefore enabled for Unity Catalog.

Method 2: Run a SQL query to confirm Unity Catalog enablement
Run the following SQL query in the SQL query editor or a notebook that is attached to a Unity Catalog-enabled compute resource. No admin role is required.

```
SELECT CURRENT_METASTORE();
```

If the query returns a metastore ID like the following, then your workspace is attached to a Unity Catalog metastore and therefore enabled for Unity Catalog.

Remediation:

Use the remediation procedure written in this article: https://learn.microsoft.com/en-us/azure/databricks/data-governance/unity-catalog/get-started.

Default Value:

New workspaces have Unity Catalog enabled by default. Existing workspaces may require manual enablement.

References:

1. https://learn.microsoft.com/en-us/azure/databricks/data-governance/unity-catalog/
2. https://learn.microsoft.com/en-us/azure/databricks/admin/users-groups/
3. https://learn.microsoft.com/en-us/azure/databricks/data-governance/unity-catalog/enable-workspaces

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

3.1.6 Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens (Manual)

Profile Applicability:

- Level 1

Description:

Databricks personal access tokens (PATs) provide API-based authentication for users and applications. By default, users can generate API tokens without expiration, leading to potential security risks if tokens are leaked, improperly stored, or not rotated regularly.

To mitigate these risks, administrators should:

- Restrict token creation to approved users and service principals.
- Enforce expiration policies to prevent long-lived tokens.
- Monitor token usage and revoke unused or compromised tokens.

Rationale:

Restricting usage and enforcing expiry for personal access tokens reduces exposure to long-lived tokens, minimizes the risk of API abuse if compromised, and aligns with security best practices through controlled issuance and enforced expiry.

Impact:

If revoked improperly, applications relying on these tokens may fail, requiring a remediation plan for token rotation. Increased administrative effort is required to track and manage API tokens effectively.

Audit:

Azure Databricks administrators can monitor and revoke personal access tokens within their workspace. Detailed instructions are available in the "Monitor and Revoke Personal Access Tokens" section of the Microsoft documentation: https://learn.microsoft.com/en-us/azure/databricks/admin/access-control/tokens.
To evaluate the usage of personal access tokens in your Azure Databricks account, you can utilize the provided notebook that lists all PATs not rotated or updated in the last 90 days, allowing you to identify tokens that may require revocation. This process is detailed here: https://docs.azure.cn/en-us/databricks/security/auth/oauth-pat-usage.
Implementing diagnostic logging provides a comprehensive reference of audit log services and events, enabling you to track activities related to personal access tokens. More information can be found in the diagnostic log reference section: https://docs.azure.cn/en-us/databricks/security/auth/oauth-pat-usage.

Remediation:

Remediate from Azure Portal
Disable personal access tokens:
If your workspace does not require PATs, you can disable them entirely to prevent their use.

1. Navigate to your Azure Databricks workspace.
2. Click the `Settings` icon and select `Admin Console`.
3. Go to the `Advanced` tab.
4. Under `Personal Access Tokens`, toggle the setting to `Disabled`.

Databricks CLI:

```
databricks workspace-conf set-status --json '{"enableTokens": "false"}'
```

Control who can create and use personal access tokens:
Define which users or groups are authorized to create and utilize PATs.

1. Navigate to your Azure Databricks workspace.
2. Click the `Settings` icon and select `Admin Console`.
3. Go to the `Advanced` tab.
4. Click on `Personal Access Tokens` and then `Permissions`.
5. Assign the appropriate permissions (e.g. No Permissions, Can Use, Can Manage) to users or groups.

Set maximum lifetime for new personal access tokens:
Limit the validity period of new tokens to reduce potential misuse.
Databricks CLI:

```
databricks workspace-conf set-status --json '{"maxTokenLifetimeDays": "90"}'
```

Monitor and revoke personal access tokens:
Periodically review active tokens and revoke any that are unnecessary or potentially compromised.
Databricks CLI:

```
databricks token list
databricks token delete --token-id <token-id>
```

Transition to OAuth for enhanced security:
Utilize OAuth tokens for authentication, offering improved security features over PATs.

Default Value:

By default, personal access tokens are enabled and users can create the Personal access token and their expiry time.

References:

1. https://learn.microsoft.com/en-us/azure/databricks/administration-guide/access-control/tokens

2. https://learn.microsoft.com/en-us/azure/databricks/dev-tools/auth/

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.		●	●

3.1.7 Ensure that diagnostic log delivery is configured for Azure Databricks (Manual)

Profile Applicability:

- Level 1

Description:

Azure Databricks Diagnostic Logging provides insights into system operations, user activities, and security events within a Databricks workspace. Enabling diagnostic logs helps organizations:

- Detect security threats by logging access, job executions, and cluster activities.
- Ensure compliance with industry regulations such as SOC 2, HIPAA, and GDPR.
- Monitor operational performance and troubleshoot issues proactively.

Rationale:

Diagnostic logging provides visibility into security and operational activities within Databricks workspaces while maintaining an audit trail for forensic investigations, and it supports compliance with regulatory standards that require logging and monitoring.

Impact:

Logs consume storage and may require additional monitoring tools, leading to increased operational overhead and costs. Incomplete log configurations may result in missing critical events, reducing monitoring effectiveness.

Audit:

Audit from Azure Portal
Check if diagnostic logging is enabled for the Databricks workspace:

1. Go to `Azure Databricks`.
2. Select a workspace.
3. In the left-hand menu, select `Monitoring` > `Diagnostic settings`.
4. Verify if a diagnostic setting is configured. If not, diagnostic logging is not enabled.

Ensure that logging is enabled for the following categories:

- `Audit Logs`: User and system activities.
- `Cluster Logs`: Cluster state changes and errors.
- `Notebook Logs`: Execution events.
- `Jobs Logs`: Job execution tracking.

Verify that logs are being sent to one or more of the following destinations:

- `Azure Log Analytics workspace`: For analysis and querying.
- `Azure Storage Account`: For long-term retention.
- `Azure Event Hubs`: For integration with SIEM tools.

Audit from Azure CLI
Check if diagnostic logging is enabled for the Databricks workspace:

```
az monitor diagnostic-settings list --resource <databricks-resource-id>
```

If the output is empty, no diagnostic settings are configured.
Verify log categories being collected:

```
az monitor diagnostic-settings show --name <setting-name> --resource
<databricks-resource-id>
```

Review the output to confirm that the necessary log categories are enabled.
Check if logs are stored securely in an approved location:

```
az monitor diagnostic-settings list --resource <databricks-resource-id>
```

Review the storageAccountId, workspaceId, and eventHubAuthorizationRuleId fields in the output to confirm the log destinations.
Audit from PowerShell
Check if diagnostic logging is enabled for the Databricks workspace:

```
Get-AzDiagnosticSetting -ResourceId <databricks-resource-id>
```

An empty result indicates that diagnostic logging is not enabled.

Remediation:

Remediate from Azure Portal
Enable diagnostic logging for Azure Databricks:

1. Navigate to your Azure Databricks workspace.
2. In the left-hand menu, select `Monitoring` > `Diagnostic settings`.
3. Click `+ Add diagnostic setting`.
4. Under `Category details`, select the log categories you wish to capture, such as AuditLogs, Clusters, Notebooks, and Jobs.
5. Choose a destination for the logs:
    - `Log Analytics workspace`: For advanced querying and monitoring.
    - `Storage account`: For long-term retention.
    - `Event Hub`: For integration with third-party systems.
6. Provide a `Name` for the diagnostic setting.
7. Click `Save`.

Implement log retention policies:

1. Navigate to your Log Analytics workspace.
2. Under `General`, select `Usage and estimated costs`.

3. Click `Data Retention`.
4. Adjust the retention period slider to the desired number of days (up to 730 days).
5. Click `OK`.

Monitor logs for anomalies:

1. Navigate to `Azure Monitor`.
2. Select `Alerts` > `+ New alert rule`.
3. Under `Scope`, specify the Databricks resource.
4. Define `Condition` based on log queries that identify anomalies (e.g. unauthorized access attempts).
5. Configure `Actions` to notify stakeholders or trigger automated responses.
6. Provide an Alert rule `name` and `description`.
7. Click `Create alert rule`.

Remediate from Azure CLI

Enable diagnostic logging for Azure Databricks:

```
az monitor diagnostic-settings create --name "DatabricksLogging" --resource
<databricks-resource-id> --logs '[{"category": "AuditLogs", "enabled": true},
{"category": "Clusters", "enabled": true}, {"category": "Notebooks",
"enabled": true}, {"category": "Jobs", "enabled": true}]' --workspace <log-
analytics-id>
```

Implement log retention policies:

```
az monitor log-analytics workspace update --resource-group <resource-group> -
-name <log-analytics-name> --retention-time 365
```

Monitor logs for anomalies:

```
az monitor activity-log alert create --name "DatabricksAnomalyAlert" --
resource-group <resource-group> --scopes <databricks-resource-id> --condition
"contains 'UnauthorizedAccess'"
```

References:

1. https://learn.microsoft.com/en-us/azure/databricks/admin/account-settings/audit-log-delivery
2. https://learn.microsoft.com/en-us/troubleshoot/azure/azure-monitor/log-analytics/billing/configure-data-retention

Additional Information:

- Ensure that the Azure Databricks workspace is on the Premium plan to utilize diagnostic logging features.
- Regularly review and update alert rules to adapt to evolving security threats and operational requirements.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

3.1.8 Ensure that data at rest and in transit is encrypted in Azure Databricks using customer managed keys (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Azure Databricks encrypts data in transit using TLS 1.2+ to secure API, workspace, and cluster communications. By default, data at rest is encrypted using Microsoft-managed keys.

Rationale:

Organizations with stricter needs for control of encryption keys should enable customer-managed keys (CMK) for greater control over data encryption, auditing, and regulatory compliance. Azure Key Vault should be used to store and manage CMKs.

Enforcing encryption at rest and in transit in Azure Databricks:

- Protects sensitive data from unauthorized access.
- Ensures regulatory compliance (ISO 27001, GDPR, HIPAA, SOC 2).
- Allows key revocation and rotation control with customer-managed keys (CMK).
- Mitigates insider threats by preventing unauthorized access to raw storage.

Impact:

Enabling CMK encryption requires additional configuration. Key management introduces maintenance overhead (rotation, revocation, lifecycle management). Potential access issues will be encountered if keys are deleted or rotated incorrectly.

Audit:

Audit from Azure Portal

1. Go to Azure Portal → Databricks Workspaces.
2. Select a Databricks Workspace and go to Encryption settings.
3. Check if customer-managed keys (CMK) are enabled under "Managed Disk Encryption".
4. If CMK is not enabled, the workspace is non-compliant.

Audit from Azure CLI

Run the following command to check encryption settings for Databricks workspace:

```
az databricks workspace show --name <databricks-workspace-name> --resource-group <resource-group-name> --query encryption
```

Ensure that keySource is set to `Microsoft.KeyVault`.

Audit from PowerShell

```
Get-AzDatabricksWorkspace -ResourceGroupName "<resource-group-name>" -Name
"<databricks-workspace-name>" | Select-Object Encryption
```

Verify that encryption is set to `Customer-Managed Keys (CMK)`.

Audit from Databricks CLI

```
databricks workspace get-metadata --workspace-id <workspace-id>
```

Ensure that encryption settings reflect a CMK setup.

Remediation:

NOTE: These remediations assume that an Azure KeyVault already exists in the subscription.

Remediate from Azure CLI

1. Create a dedicated key:

```
az keyvault key create --vault-name <keyvault-name> --name <key-name> --
protection <"software" or "hsm">
```

2. Assign permissions to Databricks:

```
az keyvault set-policy --name <keyvault-name> --resource-group <resource-
group-name> --spn <databricks-spn> --key-permissions get wrapKey unwrapKey
```

3. Enable encryption with CMK:

```
az databricks workspace update --name <databricks-workspace-name> --resource-
group <resource-group-name> --key-source "Microsoft.KeyVault" --key-name
<key-name> --keyvault-uri <keyvault-uri>
```

Remediate from PowerShell

```
$Key = Add-AzKeyVaultKey -VaultName <keyvault-name> -Name <key-name> -
Destination <"software" or "hsm">
Set-AzDatabricksWorkspace -ResourceGroupName "<resource-group-name>" -
WorkspaceName "<databricks-workspace-name>" -EncryptionKeySource
"Microsoft.KeyVault" -KeyVaultUri $Key.Id
```

Default Value:

By default, Azure Databricks uses Microsoft-managed keys for encryption. Data in transit is always encrypted using TLS 1.2+. Customer-Managed Keys (CMK) must be manually enabled.

CIS Controls:

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

4 Compute Services

SERVICE CATEGORY BENCHMARK AVAILABLE:

- "CIS Microsoft Azure Compute Services Benchmark"

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

PARTIAL RELOCATION - BE ADVISED!

Some recommendations previously covered in the CIS Microsoft Azure Foundations Benchmark (this document) related to Compute services have been relocated to a Benchmark titled **CIS Microsoft Azure Compute Services Benchmark**. This Compute Services section now provides a **foundational set** of secure configuration recommendations for products from Azure Product Directory's "Compute" category of services.

After applying foundational recommendations, take inventory of the entire set of Compute Services in use by your organization, then look to the Benchmarks section of the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72) for defense-in-depth guidance for those specific services in the **CIS Microsoft Azure Compute Services Benchmark**.

Services addressed in the **CIS Microsoft Azure Compute Services Benchmark**:

- App Service
- Azure Container Instances
- Azure CycleCloud
- Azure Dedicated Host
- Azure Functions
- Azure Kubernetes Service (AKS)
- Azure Quantum
- Azure Service Fabric
- Azure Spot Virtual Machines
- Azure Spring Apps
- Azure Virtual Desktop
- Azure VM Image Builder
- Azure VMware Solution
- Batch
- Cloud Services
- Linux Virtual Machines
- SQL Server on Azure Virtual Machines
- Static Web Apps
- Virtual Machine Scale Sets
- Virtual Machines

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#compute

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

4.1 Virtual Machines

This section covers security recommendations to follow for the configuration of Virtual Machines on an Azure subscription.

4.1.1 Ensure only MFA enabled identities can access privileged Virtual Machine (Manual)

Profile Applicability:

- Level 2

Description:

Verify identities without MFA that can log in to a privileged virtual machine using separate login credentials. An adversary can leverage the access to move laterally and perform actions with the virtual machine's managed identity. Make sure the virtual machine only has necessary permissions, and revoke the admin-level permissions according to the principle of least privilege.

Rationale:

Integrating multi-factor authentication (MFA) as part of the organizational policy can greatly reduce the risk of an identity gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs.

An Adversary may log into accessible cloud services within a compromised environment using Valid Accounts that are synchronized to move laterally and perform actions with the virtual machine's managed identity. The adversary may then perform management actions or access cloud-hosted resources as the logged-on managed identity.

Impact:

This recommendation requires the Entra ID P2 license to implement.

Ensure that identities provisioned to a virtual machine utilize an RBAC/ABAC group and are allocated a role using Azure PIM, and that the role settings require MFA or use another third-party PAM solution for accessing virtual machines.

Audit:

Audit from Azure Portal

1. Log in to the Azure portal.
2. Select the `Subscription`, then click on `Access control (IAM)`.
3. Click `Role : All` and click `All` to display the drop-down menu.
4. Type `Virtual Machine Administrator Login` and select `Virtual Machine Administrator Login`.
5. Review the list of identities that have been assigned the `Virtual Machine Administrator Login` role.
6. Go to `Microsoft Entra ID`.
7. For `Per-user MFA`:
    a) Under `Manage`, click `Users`.

b) Click Per-user MFA.
c) Ensure that none of the identities assigned the Virtual Machine Administrator Login role from step 4 have Status set to disabled.

8. For Conditional Access:
   a) Under Manage, click Security.
   b) Under Protect, click Conditional Access.
   c) Ensure that none of the identities assigned the Virtual Machine Administrator Login role from step 4 are exempt from a Conditional Access policy requiring MFA for all users.

Remediation:

Remediate from Azure Portal

1. Log in to the Azure portal.
2. This can be remediated by enabling MFA for user, Removing user access or Reducing access of managed identities attached to virtual machines.

Case I : Enable MFA for users having access on virtual machines.

1. Go to Microsoft Entra ID.
2. For Per-user MFA:
   a) Under Manage, click Users.
   b) Click Per-user MFA.
   c) For each user requiring remediation, check the box next to their name.
   d) Click Enable MFA, then Click Enable.
3. For Conditional Access:
   a) Under Manage, click Security.
   b) Under Protect, click Conditional Access.
   c) Update the Conditional Access policy requiring MFA for all users, removing each user requiring remediation from the Exclude list.

Case II : Removing user access on a virtual machine.

1. Select the Subscription, then click on Access control (IAM).
2. Select Role assignments and search for Virtual Machine Administrator Login or Virtual Machine User Login or any role that provides access to log into virtual machines.
3. Click on Role Name, Select Assignments, and remove identities with no MFA configured.

Case III : Reducing access of managed identities attached to virtual machines.

1. Select the Subscription, then click on Access control (IAM).
2. Select Role Assignments from the top menu and apply filters on Assignment type as Privileged administrator roles and Type as Virtual Machines.
3. Click on Role Name, Select Assignments, and remove identities access make sure this follows the least privileges principal.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.002, T1078.004		

5 Database Services (reference)

SERVICE CATEGORY BENCHMARK AVAILABLE:

- "CIS Microsoft Azure Database Services Benchmark"

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

`FULL RELOCATION - BE ADVISED!`

- ALL - recommendations previously covered in the CIS Microsoft Azure Foundations Benchmark (this document) related to products in the Database category of services have been relocated to a Benchmark titled **CIS Microsoft Azure Database Services Benchmark**. This section now serves only as a reference.

Services addressed in the **CIS Microsoft Azure Database Services Benchmark**:

- Azure Cache for Redis
- Azure Cosmos DB
- Azure Data Factory
- Azure Database for MariaDB
- Azure Database for MySQL
- Azure Database for PostgreSQL
- Azure Database Migration Service
- Azure SQL
- Azure SQL Database
- Azure SQL Edge
- Azure SQL Managed Instance
- SQL Server on Azure Virtual Machines
- Table Storage
- Azure Managed Instance for Apache Cassandra
- Azure confidential ledger

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#databases

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

6 Identity Services

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

This section covers security best practice recommendations for products in the Azure Identity services category.

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#identity

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

6.1 Security Defaults (Per-User MFA)

IMPORTANT: READ BELOW BEFORE PROCEEDING!

- If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, F5, or Business Premium, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.
- If your organization is using the free tier of Entra ID (Office 365 E1, E3, or E5, and Microsoft 365 F1 or F3 licenses) and **CAN NOT** use Conditional Access, proceed with the Security Defaults guidance in this section, and ignore the recommendations in the Conditional Access section.

Conditional Access is preferred, but Security Defaults (Per-User MFA) is recommended only if Conditional Access isn't available.

Why is this **IMPORTANT**?

The Azure "Security Defaults" recommendations represent an entry-level set of recommendations (such as Multi-Factor Authentication) which will be relevant to organizations and tenants that are either just starting to use Azure, or are only utilizing a bare minimum feature set, and rely on the free license tier of Microsoft Entra ID. Security Defaults recommendations are intended to ensure that these use cases are still capable of establishing a strong baseline of secure configuration.

If your subscription is licensed to use Microsoft Entra ID P1 or P2, it is strongly recommended that the "Security Defaults" section (this section and the recommendations therein) be bypassed in favor of the use of "Conditional Access."

IMPORTANT: READ ABOVE BEFORE PROCEEDING!

6.1.1 Ensure that 'security defaults' is enabled in Microsoft Entra ID (Manual)

Profile Applicability:

- Level 1

Description:

[**IMPORTANT - Please read the section overview:** If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, F5, or Business Premium, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.]

Security defaults in Microsoft Entra ID make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks.

Security defaults is available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. You may turn on security defaults in the Azure portal.

Rationale:

Security defaults provide secure default settings that we manage on behalf of organizations to keep customers safe until they are ready to manage their own identity security settings.

For example, doing the following:

- Requiring all users and admins to register for MFA.
- Challenging users with MFA - when necessary, based on factors such as location, device, role, and task.
- Disabling authentication from legacy authentication clients, which can’t do MFA.

Impact:

This recommendation should be implemented initially and then may be overridden by other service/product specific CIS Benchmarks. Administrators should also be aware that certain configurations in Microsoft Entra ID may impact other Microsoft services such as Microsoft 365.

Audit:

Audit from Azure Portal
To ensure security defaults is enabled in your directory:

1. From Azure Home select the Portal Menu.
2. Browse to `Microsoft Entra ID` > `Properties`.

3. Select `Manage security defaults`.
4. Under `Security defaults`, verify that `Enabled (recommended)` is selected.

Remediation:

Remediate from Azure Portal
To enable security defaults in your directory:

1. From Azure Home select the Portal Menu.
2. Browse to `Microsoft Entra ID` > `Properties`.
3. Select `Manage security defaults`.
4. Under `Security defaults`, select `Enabled (recommended)`.
5. Select `Save`.

Default Value:

If your tenant was created on or after October 22, 2019, security defaults may already be enabled in your tenant.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
2. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-2-protect-identity-and-authentication-systems

Additional Information:

This recommendation differs from the Microsoft 365 Benchmark. This is because the potential impact associated with disabling Security Defaults is dependent upon the security settings implemented in the environment. It is recommended that organizations disabling Security Defaults implement appropriate security settings to replace the settings configured by Security Defaults.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.1.2 Ensure that 'multifactor authentication' is 'enabled' for all users (Manual)

Profile Applicability:

- Level 1

Description:

[**IMPORTANT - Please read the section overview:** If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, F5, or Business Premium, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.]

Enable multifactor authentication for all users.

Note: Since 2024, Azure has been rolling out mandatory multifactor authentication. For more information:

- https://azure.microsoft.com/en-us/blog/announcing-mandatory-multi-factor-authentication-for-azure-sign-in
- https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication

Rationale:

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Users would require two forms of authentication before any access is granted. Additional administrative time will be required for managing dual forms of authentication when enabling multifactor authentication.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Entra ID`.
2. Under `Manage`, click `Users`.
3. Click `Per-user MFA` from the top menu.
4. Ensure that `Status` is `enabled` for all users.

Audit from REST API

Run the following Graph PowerShell command:

```
get-mguser -All | where {$_.StrongAuthenticationMethods.Count -eq 0} |
Select-Object -Property UserPrincipalName
```

If the output contains any `UserPrincipalName`, then this recommendation is non-compliant.

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Entra ID`.
2. Under `Manage`, click `Users`.
3. Click `Per-user MFA` from the top menu.
4. Click the box next to a user with `Status disabled`.
5. Click `Enable MFA`.
6. Click `Enable`.
7. Repeat steps 1-6 for each user requiring remediation.

Other options within Azure Portal

- https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa
- https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings
- https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa
- https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted#enable-multi-factor-authentication-with-conditional-access

Default Value:

Multifactor authentication is not enabled for all users by default. Starting in 2024, multifactor authentication is enabled for administrative accounts by default.

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication
3. https://azure.microsoft.com/en-us/blog/announcing-mandatory-multi-factor-authentication-for-azure-sign-in/
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-4-authenticate-server-and-services

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1032

6.1.3 Ensure that 'Allow users to remember multifactor authentication on devices they trust' is disabled (Manual)

Profile Applicability:

- Level 1

Description:

[**IMPORTANT - Please read the section overview:** If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, F5, or Business Premium, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.]

Do not allow users to remember multi-factor authentication on devices.

Rationale:

Remembering Multi-Factor Authentication (MFA) for devices and browsers allows users to have the option to bypass MFA for a set number of days after performing a successful sign-in using MFA. This can enhance usability by minimizing the number of times a user may need to perform two-step verification on the same device. However, if an account or device is compromised, remembering MFA for trusted devices may affect security. Hence, it is recommended that users not be allowed to bypass MFA.

Impact:

For every login attempt, the user will be required to perform multi-factor authentication.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, click `Users`
4. Click the `Per-user MFA` button on the top bar
5. Click on `Service settings`
6. Ensure that `Allow users to remember multi-factor authentication on devices they trust` is not enabled

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, click `Users`

4. Click the `Per-user MFA` button on the top bar
5. Click on `Service settings`
6. Uncheck the box next to `Allow users to remember multi-factor authentication on devices they trust`
7. Click `Save`

Default Value:

By default, `Allow users to remember multi-factor authentication on devices they trust` is disabled.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication-for-devices-that-users-trust
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1032

6.2 Conditional Access

For most Azure tenants, and certainly for organizations with a significant use of Microsoft Entra ID, Conditional Access policies are recommended and preferred. To use Conditional Access Policies, a licensing plan is required, and **Security Defaults must be disabled**. Because of the licensing requirement, all Conditional Access policies are assigned a profile of "Level 2."

Conditional Access requires one of the following plans:

- Microsoft Entra ID P1 or P2
- Microsoft 365 Business Premium
- Microsoft 365 E3 or E5
- Microsoft 365 F1, F3, F5 Security and F5 Security + Compliance
- Enterprise Mobility & Security E3 or E5

6.2.1 Ensure that 'trusted locations' are defined (Manual)

Profile Applicability:

- Level 2

Description:

Microsoft Entra ID Conditional Access allows an organization to configure `Named locations` and configure whether those locations are trusted or untrusted. These settings provide organizations the means to specify Geographical locations for use in conditional access policies, or define actual IP addresses and IP ranges and whether or not those IP addresses and/or ranges are trusted by the organization.

Rationale:

Defining trusted source IP addresses or ranges helps organizations create and enforce Conditional Access policies around those trusted or untrusted IP addresses and ranges. Users authenticating from trusted IP addresses and/or ranges may have less access restrictions or access requirements when compared to users that try to authenticate to Microsoft Entra ID from untrusted locations or untrusted source IP addresses/ranges.

Impact:

When configuring `Named locations`, the organization can create locations using Geographical location data or by defining source IP addresses or ranges. Configuring `Named locations` using a Country location does not provide the organization the ability to mark those locations as trusted, and any Conditional Access policy relying on those `Countries location` setting will not be able to use the `All trusted locations` setting within the Conditional Access policy. They instead will have to rely on the `Select locations` setting. This may add additional resource requirements when configuring and will require thorough organizational testing.

In general, Conditional Access policies may completely prevent users from authenticating to Microsoft Entra ID, and thorough testing is recommended. To avoid complete lockout, a 'Break Glass' account with full Global Administrator rights is recommended in the event all other administrators are locked out of authenticating to Microsoft Entra ID. This 'Break Glass' account should be excluded from Conditional Access Policies and should be configured with the longest pass phrase feasible in addition to a FIDO2 security key or certificate kept in a very secure physical location. This account should only be used in the event of an emergency and complete administrator lockout.

NOTE: Starting July 2024, Microsoft will begin requiring MFA for All Users - including Break Glass Accounts. By the end of October 2024, this requirement will be enforced. Physical FIDO2 security keys, or a certificate kept on secure removable storage can fulfill this MFA requirement. If opting for a physical device, that device should be kept in a very secure, documented physical location.

Audit:

Audit from Azure Portal

1. In the Azure Portal, navigate to `Microsoft Entra ID`
2. Under `Manage`, click `Security`
3. Under `Protect`, click `Conditional Access`
4. Under `Manage`, click `Named locations`

Ensure there are `IP ranges location` settings configured and marked as `Trusted`

Audit from PowerShell

```
Get-MgIdentityConditionalAccessNamedLocation
```

In the output from the above command, for each Named location group, make sure at least one entry contains the `IsTrusted` parameter with a value of `True`. Otherwise, if there is no output as a result of the above command or all of the entries contain the `IsTrusted` parameter with an empty value, a `NULL` value, or a value of `False`, the results are out of compliance with this check.

Remediation:

Remediate from Azure Portal

1. In the Azure Portal, navigate to `Microsoft Entra ID`
2. Under `Manage`, click `Security`
3. Under `Protect`, click `Conditional Access`
4. Under `Manage`, click `Named locations`
5. Within the `Named locations` blade, click on `IP ranges location`
6. Enter a name for this location setting in the `Name` text box
7. Click on the `+` sign
8. Add an IP Address Range in CIDR notation inside the text box that appears
9. Click on the `Add` button
10. Repeat steps 7 through 9 for each IP Range that needs to be added
11. If the information entered are trusted ranges, select the `Mark as trusted location` check box
12. Once finished, click on `Create`

Remediate from PowerShell
Create a new trusted IP-based Named location policy

```
[System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.IpRange]]$ipR
anges = @()
$ipRanges.Add("<first IP range in CIDR notation>")
$ipRanges.Add("<second IP range in CIDR notation>")
$ipRanges.Add("<third IP range in CIDR notation>")
New-MgIdentityConditionalAccessNamedLocation -dataType
"#microsoft.graph.ipNamedLocation" -DisplayName "<name of IP Named location
policy>" -IsTrusted $true -IpRanges $ipRanges
```

Set an existing IP-based Named location policy to trusted *[next page]*

```
Update-MgIdentityConditionalAccessNamedLocation -PolicyId "<ID of the
policy>" -dataType "#microsoft.graph.ipNamedLocation" -IsTrusted $true
```

Default Value:

By default, no locations are configured under the `Named locations` blade within the Microsoft Entra ID Conditional Access blade.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
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	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098.001	TA0001	M1030

6.2.2 Ensure that an exclusionary geographic Conditional Access policy is considered (Manual)

Profile Applicability:

- Level 2

Description:

CAUTION: If these policies are created without first auditing and testing the result, misconfiguration can potentially lock out administrators or create undesired access issues.

Conditional Access Policies can be used to block access from geographic locations that are deemed out-of-scope for your organization or application. The scope and variables for this policy should be carefully examined and defined.

Rationale:

Conditional Access, when used as a deny list for the tenant or subscription, is able to prevent ingress or egress of traffic to countries that are outside of the scope of interest (e.g.: customers, suppliers) or jurisdiction of an organization. This is an effective way to prevent unnecessary and long-lasting exposure to international threats such as APTs.

Impact:

Microsoft Entra ID P1 or P2 is required. Limiting access geographically will deny access to users that are traveling or working remotely in a different part of the world. A point-to-site or site to site tunnel such as a VPN is recommended to address exceptions to geographic access policies.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal menu in the top left, and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit, then:
    - Under `Assignments` > `Users`, review the users and groups for the personnel the policy will apply to
    - Under `Assignments` > `Target resources`, review the cloud apps or actions for the systems the policy will apply to
    - Under `Conditions` > `Locations`, Review the `Include` locations for those that should be **blocked**

- Under Conditions > Locations, Review the Exclude locations for those that should be allowed (Note: locations set up in the previous recommendation for Trusted Location should be in the Exclude list.)
- Under Access Controls > Grant - Confirm that Block access is selected.

Audit from Azure CLI

```
As of this writing there are no subcommands for Conditional Access Policies
within the Azure CLI
```

Audit from PowerShell

```
$conditionalAccessPolicies = Get-MgIdentityConditionalAccessPolicy

foreach($policy in $conditionalAccessPolicies) {$policy | Select-Object
@{N='Policy ID'; E={$policy.id}}, @{N="Included Locations";
E={$policy.Conditions.Locations.IncludeLocations}}, @{N="Excluded Locations";
E={$policy.Conditions.Locations.ExcludeLocations}}, @{N="BuiltIn
GrantControls"; E={$policy.GrantControls.BuiltInControls}}}
```

Make sure there is at least 1 row in the output of the above PowerShell command that contains Block under the BuiltIn GrantControls column and location IDs under the Included Locations and Excluded Locations columns. If not, a policy containing these options has not been created and is considered a finding.

Remediation:

Remediate from Azure Portal

Part 1 of 2 - Create the policy and enable it in Report-only mode.

1. From Azure Home open the portal menu in the top left, and select Microsoft Entra ID.
2. Scroll down in the menu on the left, and select Security.
3. Select on the left side Conditional Access.
4. Select Policies.
5. Click the + New policy button, then:
6. Provide a name for the policy.
7. Under Assignments, select Users then:
   - Under Include, select All users
   - Under Exclude, check Users and groups and only select emergency access accounts and service accounts (**NOTE**: Service accounts are excluded here because service accounts are non-interactive and cannot complete MFA)
8. Under Assignments, select Target resources then:
   - Under Include, select All cloud apps
   - Leave Exclude blank unless you have a well defined exception
9. Under Conditions, select Locations then:
   - Select Include, then add entries for locations for those that should be **blocked**

    - Select `Exclude`, then add entries for those that should be allowed (**IMPORTANT**: Ensure that all Trusted Locations are in the `Exclude` list.)
10. Under `Access Controls`, select `Grant` select `Block Access`.
11. Set `Enable policy` to `Report-only`.
12. Click `Create`.

Allow some time to pass to ensure the sign-in logs capture relevant conditional access events. These events will need to be reviewed to determine if additional considerations are necessary for your organization (e.g. legitimate locations are being blocked and investigation is needed for exception).
NOTE: The policy is not yet 'live,' since `Report-only` is being used to audit the effect of the policy.
Part 2 of 2 - Confirm that the policy is not blocking access that should be granted, then toggle to `On`.

1. With your policy now in report-only mode, return to the Microsoft Entra blade and click on `Sign-in logs`.
2. Review the recent sign-in events - click an event then review the event details (specifically the `Report-only` tab) to ensure:
    - The sign-in event you're reviewing occurred **after** turning on the policy in report-only mode
    - The policy name from step 6 above is listed in the `Policy Name` column
    - The `Result` column for the new policy shows that the policy was `Not applied` (indicating the location origin was not blocked)
3. If the above conditions are present, navigate back to the policy name in Conditional Access and open it.
4. Toggle the policy from `Report-only` to `On`.
5. Click `Save`.

Remediate from PowerShell
First, set up the conditions objects values before updating an existing conditional access policy or before creating a new one. You may need to use additional PowerShell cmdlets to retrieve specific IDs such as the `Get-MgIdentityConditionalAccessNamedLocation` which outputs the `Location IDs` for use with conditional access policies.

```
$conditions = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessConditionSet

$conditions.Applications = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessApplicationCondition
$conditions.Applications.IncludeApplications = <"All" | "Office365" | "app
ID" | @("app ID 1", "app ID 2", etc...>
$conditions.Applications.ExcludeApplications = <"Office365" | "app ID" |
@("app ID 1", "app ID 2", etc...)>

$conditions.Users = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessUserCondition
$conditions.Users.IncludeUsers = <"All" | "None" | "GuestsOrExternalUsers" |
"Specific User ID" | @("User ID 1", "User ID 2", etc.)>
$conditions.Users.ExcludeUsers = <"GuestsOrExternalUsers" | "Specific User
ID" | @("User ID 1", "User ID 2", etc.)>
$conditions.Users.IncludeGroups = <"group ID" | "All" | @("Group ID 1",
"Group ID 2", etc...)>
$conditions.Users.ExcludeGroups = <"group ID" | @("Group ID 1", "Group ID 2",
etc...)>
$conditions.Users.IncludeRoles = <"Role ID" | "All" | @("Role ID 1", "Role ID
2", etc...)>
$conditions.Users.ExcludeRoles = <"Role ID" | @("Role ID 1", "Role ID 2",
etc...)>

$conditions.Locations = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessLocationCondition
$conditions.Locations.IncludeLocations = <"Location ID" | @("Location ID 1",
"Location ID 2", etc...) >
$conditions.Locations.ExcludeLocations = <"AllTrusted" | "Location ID" |
@("Location ID 1", "Location ID 2", etc...)>


$controls = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessGrantControls
$controls._Operator = "OR"
$controls.BuiltInControls = "block"
```

Next, update the existing conditional access policy with the condition set options configured with the previous commands.

```
Update-MgIdentityConditionalAccessPolicy -PolicyId <policy ID> -Conditions
$conditions -GrantControls $controls
```

To create a new conditional access policy that complies with this best practice, run the following commands after creating the condition set above

```
New-MgIdentityConditionalAccessPolicy -Name "Policy Name" -State
<enabled|disabled> -Conditions $conditions -GrantControls $controls
```

Default Value:

This policy does not exist by default.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location
2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098.001	TA0001	M1030

6.2.3 Ensure that an exclusionary device code flow policy is considered (Manual)

Profile Applicability:

- Level 2

Description:

Conditional Access Policies can be used to prevent the Device code authentication flow. Device code flow should be permitted only for users that regularly perform duties that explicitly require the use of Device Code to authenticate, such as utilizing Azure with PowerShell.

Rationale:

Attackers use Device code flow in phishing attacks and, if successful, results in the attacker gaining access tokens and refresh tokens which are scoped to "user_impersonation", which can perform any action the user has permission to perform.

Impact:

Microsoft Entra ID P1 or P2 is required.

This policy should be tested using the `Report-only mode` before implementation. Without a full and careful understanding of the accounts and personnel who require Device code authentication flow, implementing this policy can block authentication for users and devices who rely on Device code flow. For users and devices that rely on device code flow authentication, more secure alternatives should be implemented wherever possible.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal menu in the top left and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit, then:
    - Under `Assignments` > `Users`, review the users and groups for the personnel the policy will apply to
    - Under `Assignments` > `Target resources`, review the cloud apps or actions for the systems the policy will apply to
    - Under `Conditions` > `Authentication Flows`, review the configuration to ensure `Device code flow` is selected

- Under `Access Controls` > `Grant` - Confirm that `Block access` is selected.

Remediation:

Remediate from Azure Portal
Part 1 of 2 - Create the policy and enable it in `Report-only` mode.

1. From Azure Home open the portal menu in the top left and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Click the `+ New policy` button, then:
6. Provide a name for the policy.
7. Under `Assignments`, select `Users` then:
   - Under `Include`, select `All users`
   - Under `Exclude`, check Users and groups and only select emergency access accounts
8. Under `Assignments`, select `Target resources` then:
   - Under `Include`, select `All cloud apps`
   - Leave `Exclude` blank unless you have a well defined exception
9. Under `Conditions` > `Authentication Flows`, set Configure to `Yes` then:
   - Select `Device code flow`
   - Select `Done`
10. Under `Access Controls` > `Grant`, select `Block Access`.
11. Set `Enable policy` to `Report-only`.
12. Click `Create`.

Allow some time to pass to ensure the sign-in logs capture relevant conditional access events. These events will need to be reviewed to determine if additional considerations are necessary for your organization (e.g. many legitimate use cases of device code authentication are observed).
NOTE: The policy is not yet 'live,' since `Report-only` is being used to audit the effect of the policy.
Part 2 of 2 - Confirm that the policy is not blocking access that should be granted, then toggle to `On`.

1. With your policy now in report-only mode, return to the Microsoft Entra blade and click on `Sign-in logs`.
2. Review the recent sign-in events - click an event then review the event details (specifically the `Report-only` tab) to ensure:
   - The sign-in event you're reviewing occurred **after** turning on the policy in report-only mode
   - The policy name from step 6 above is listed in the `Policy Name` column

    - The `Result` column for the new policy shows that the policy was `Not applied` (indicating the device code authentication flow was not blocked)
3. If the above conditions are present, navigate back to the policy name in Conditional Access and open it.
4. Toggle the policy from `Report-only` to `On`.
5. Click `Save`.

Default Value:

This policy does not exist by default.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-authentication-flows#device-code-flow
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions
3. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only
4. https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-authentication-flows

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

6.2.4 Ensure that a multifactor authentication policy exists for all users (Manual)

Profile Applicability:

- Level 2

Description:

A Conditional Access policy can be enabled to ensure that users are required to use Multifactor Authentication (MFA) to login.

Note: Since 2024, Azure has been rolling out mandatory multifactor authentication. For more information:

- https://azure.microsoft.com/en-us/blog/announcing-mandatory-multi-factor-authentication-for-azure-sign-in
- https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication

Rationale:

Multifactor authentication is strongly recommended to increase the confidence that a claimed identity can be proven to be the subject of the identity. This results in a stronger authentication chain and reduced likelihood of exploitation.

Impact:

There is an increased cost associated with Conditional Access policies because of the requirement of Microsoft Entra ID P1 or P2 licenses. Additional support overhead may also need to be considered.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left, and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit.
6. Click the blue text under `Users`.
7. Under `Include` ensure that `All Users` is specified.
8. Under `Exclude` ensure that no users or groups are specified. If there are users or groups specified for exclusion, a very strong justification should exist for each exception, and all excepted account-level objects should be recorded in documentation along with the justification for comparison in future audits.

Remediation:

Remediate from Azure Portal

1. From Azure Home open Portal menu in the top left, and select `Microsoft Entra ID`.
2. Select `Security`.
3. Select `Conditional Access`.
4. Select `Policies`.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users this policy should not apply to and click `Select`.
11. Click the blue text under `Target resources`.
12. Select `All cloud apps`.
13. Click the blue text under `Grant`.
14. Under `Grant access`, check `Require multifactor authentication` and click `Select`.
15. Set `Enable policy` to `Report-only`.
16. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

Starting October 2024, MFA will be required for all accounts by default.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa
2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access-what-if
3. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in the References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1032

6.2.5 Ensure that multifactor authentication is required for risky sign-ins (Manual)

Profile Applicability:

- Level 2

Description:

Entra ID tracks the behavior of sign-in events. If the Entra ID domain is licensed with P2, the sign-in behavior can be used as a detection mechanism for additional scrutiny during the sign-in event. If this policy is set up, then Risky Sign-in events will prompt users to use multi-factor authentication (MFA) tokens on login for additional verification.

Rationale:

Enabling multi-factor authentication is a recommended setting to limit the potential of accounts being compromised and limiting access to authenticated personnel. Enabling this policy allows Entra ID's risk-detection mechanisms to force additional scrutiny on the login event, providing a deterrent response to potentially malicious sign-in events, and adding an additional authentication layer as a reaction to potentially malicious behavior.

Impact:

Risk Policies for Conditional Access require Microsoft Entra ID P2. Additional overhead to support or maintain these policies may also be required if users lose access to their MFA tokens.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu in the top left and select `Microsoft Entra ID`.
2. Select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit.
6. Click the blue text under `Users`.
7. View under `Include` the corresponding users and groups to whom the policy is applied.
8. View under `Exclude` to determine which users and groups to whom the policy is not applied.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu in the top left and select `Microsoft Entra ID`.
2. Select `Security`
3. Select `Conditional Access`.
4. Select `Policies`.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users this policy should not apply to and click `Select`.
11. Click the blue text under `Target resources`.
12. Select `All cloud apps`.
13. Click the blue text under `Conditions`.
14. Select `Sign-in risk`.
15. Update the `Configure` toggle to `Yes`.
16. Check the sign-in risk level this policy should apply to, e.g. `High` and `Medium`.
17. Select `Done`.
18. Click the blue text under `Grant` and check `Require multifactor authentication` then click the `Select` button.
19. Click the blue text under `Session` then check `Sign-in frequency` and select `Every time` and click the `Select` button.
20. Set `Enable policy` to `Report-only`.
21. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

MFA is not enabled by default.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-risk
2. https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-conditional-access-what-if
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-insights-reporting
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions
5. https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection#license-requirements

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource the in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1032

6.2.6 Ensure that multifactor authentication is required for Windows Azure Service Management API (Manual)

Profile Applicability:

- Level 2

Description:

This recommendation ensures that users accessing the Windows Azure Service Management API (i.e. Azure Powershell, Azure CLI, Azure Resource Manager API, etc.) are required to use multi-factor authentication (MFA) credentials when accessing resources through the Windows Azure Service Management API.

Rationale:

Administrative access to the Windows Azure Service Management API should be secured with a higher level of scrutiny to authenticating mechanisms. Enabling multi-factor authentication is recommended to reduce the potential for abuse of Administrative actions, and to prevent intruders or compromised admin credentials from changing administrative settings.

IMPORTANT: While this recommendation allows exceptions to specific Users or Groups, they should be very carefully tracked and reviewed for necessity on a regular interval through an Access Review process. It is important that this rule be built to include "All Users" to ensure that all users not specifically excepted will be required to use MFA to access the Azure Service Management API.

Impact:

Conditional Access policies require Microsoft Entra ID P1 or P2 licenses. Similarly, they may require additional overhead to maintain if users lose access to their MFA. Any users or groups which are granted an exception to this policy should be carefully tracked, be granted only minimal necessary privileges, and conditional access exceptions should be regularly reviewed or investigated.

Audit:

Audit from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. In the menu on the left of the Entra ID blade, click `Security`.
3. In the menu on the left of the Security blade, click `Conditional Access`.
4. In the menu on the left of the Conditional Access blade, click `Policies`.
5. Click on the name of the policy you wish to audit.
6. Click the blue text under `Users`.
7. Under the `Include` section of Users, ensure that `All Users` is selected.

8. Under the `Exclude` section of Users, review the `Users and Groups` that are excluded from the policy (NOTE: this should be limited to break-glass emergency access accounts, non-interactive service accounts, and other carefully considered exceptions).
9. On the left side, click the blue text under `Target resources`.
10. Under the `Include` section of Target Resources, ensure that the `Select apps` radio button is selected.
11. Under `Select`, ensure that `Windows Azure Service Management API` is listed.

Remediation:

Remediate from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. Click `Security` in the Entra ID blade.
3. Click `Conditional Access` in the Security blade.
4. Click `Policies` in the Conditional Access blade.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users or groups to be exempted from this policy (e.g. break-glass emergency accounts, and non-interactive service accounts) then click the `Select` button.
11. Click the blue text under `Target resources`.
12. Under `Include`, click the `Select apps` radio button.
13. Click the blue text under `Select`.
14. Check the box next to `Windows Azure Service Management APIs` then click the `Select` button.
15. Click the blue text under `Grant`.
16. Under `Grant access` check the box for `Require multi-factor authentication` then click the `Select` button.
17. Before creating, set `Enable policy` to `Report-only`.
18. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

MFA is not enabled by default for administrative actions.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-azure-management
4. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-cloud-apps#windows-azure-service-management-api

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with administrators changing settings until they use an MFA device linked to their accounts. An emergency access account is recommended for this eventuality if all administrators are locked out. Please see the documentation in the references for further information. Similarly further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1032

6.2.7 Ensure that multifactor authentication is required to access Microsoft Admin Portals (Manual)

Profile Applicability:

- Level 2

Description:

This recommendation ensures that users accessing Microsoft Admin Portals (i.e. Microsoft 365 Admin, Microsoft 365 Defender, Exchange Admin Center, Azure Portal, etc.) are required to use multi-factor authentication (MFA) credentials when logging into an Admin Portal.

Rationale:

Administrative Portals for Microsoft Azure should be secured with a higher level of scrutiny to authenticating mechanisms. Enabling multi-factor authentication is recommended to reduce the potential for abuse of Administrative actions, and to prevent intruders or compromised admin credentials from changing administrative settings.

IMPORTANT: While this recommendation allows exceptions to specific Users or Groups, they should be very carefully tracked and reviewed for necessity on a regular interval through an Access Review process. It is important that this rule be built to include "All Users" to ensure that all users not specifically excepted will be required to use MFA to access Admin Portals.

Impact:

Conditional Access policies require Microsoft Entra ID P1 or P2 licenses. Similarly, they may require additional overhead to maintain if users lose access to their MFA. Any users or groups which are granted an exception to this policy should be carefully tracked, be granted only minimal necessary privileges, and conditional access exceptions should be reviewed or investigated.

Audit:

Audit from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. In the menu on the left of the Entra ID blade, click `Security`.
3. In the menu on the left of the Security blade, click `Conditional Access`.
4. In the menu on the left of the Conditional Access blade, click `Policies`.
5. Click on the name of the policy you wish to audit.
6. Click the blue text under `Users`.
7. Under the `Include` section of Users, review `Users and Groups` to ensure that `All Users` is selected.

8. Under the `Exclude` section of Users, review the `Users and Groups` that are excluded from the policy (NOTE: this should be limited to break-glass emergency access accounts, non-interactive service accounts, and other carefully considered exceptions).
9. On the left side, click the blue text under `Target Resources`.
10. Under the `Include` section of Target resources, ensure the `Select apps` radio button is selected.
11. Under `Select`, ensure `Microsoft Admin Portals` is listed.

Remediation:

Remediate from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. Click `Security` in the Entra ID blade.
3. Click `Conditional Access` in the Security blade.
4. Click `Policies` in the Conditional Access blade.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users or groups to be exempted from this policy (e.g. break-glass emergency accounts, and non-interactive service accounts) then click the `Select` button.
11. Click the blue text under `Target resources`.
12. Under `Include`, click the `Select apps` radio button.
13. Click the blue text under `Select`.
14. Check the box next to `Microsoft Admin Portals` then click the `Select` button.
15. Click the blue text under `Grant`.
16. Under `Grant access` check the box for `Require multifactor authentication` then click the `Select` button.
17. Before creating, set `Enable policy` to `Report-only`.
18. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

MFA is not enabled by default for administrative actions.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-mfa-admin-portals

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with administrators changing settings until they use an MFA device linked to their accounts. An emergency access account is recommended for this eventuality if all administrators are locked out. Please see the documentation in the references for further information. Similarly further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1032

6.3 Periodic Identity Reviews

Security Best Practices for Identity services should include operational reviews that periodically ensure the integrity and necessity of accounts and permissions. These operational practices should be performed regularly on a cadence that is based on your organization's policy or compliance requirements.

NOTE: The recommendations in this section may not have a precise audit or remediation procedure because they may not be a configurable setting as much as they are an operative task that should be performed on a periodic basis.

6.3.1 Ensure that Azure admin accounts are not used for daily operations (Manual)

Profile Applicability:

- Level 1

Description:

Microsoft Azure admin accounts should not be used for routine, non-administrative tasks.

Rationale:

Using admin accounts for daily operations increases the risk of accidental misconfigurations and security breaches.

Impact:

Minor administrative overhead includes managing separate accounts, enforcing stricter access controls, and potential licensing costs for advanced security features.

Audit:

Audit from Azure Portal
Monitor:

1. Go to `Monitor`.
2. Click `Activity log`.
3. Review the activity log and ensure that admin accounts are not being used for daily operations.

Microsoft Entra ID:

1. Go to `Microsoft Entra ID`.
2. Under `Monitoring`, click `Sign-in logs`.
3. Review the sign-in logs and ensure that admin accounts are not being accessed more frequently than necessary.

Remediation:

If admin accounts are being used for daily operations, consider the following:

- Monitor and alert on unusual activity.
- Enforce the principle of least privilege.
- Revoke any unnecessary administrative access.
- Use Conditional Access to limit access to resources.
- Ensure that administrators have separate admin and user accounts.

- Use Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks.
- Use Privileged Identity Management (PIM) in Microsoft Entra ID to limit standing administrator access to privileged roles, discover who has access, and review privileged access.

References:

1. https://learn.microsoft.com/en-us/security/privileged-access-workstations/critical-impact-accounts

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0004	M1026

6.3.2 Ensure that guest users are reviewed on a regular basis (Manual)

Profile Applicability:

- Level 1

Description:

Microsoft Entra ID has native and extended identity functionality allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities.

Rationale:

Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely. To prevent this, guest users should be reviewed on a regular basis. During this audit, guest users should also be determined to not have administrative privileges.

Impact:

Before removing guest users, determine their use and scope. Like removing any user, there may be unforeseen consequences to systems if an account is removed without careful consideration.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Click on `Add filter`
5. Select `User type`
6. Select `Guest` from the Value dropdown
7. Click `Apply`
8. Audit the listed guest users

Audit from Azure CLI

```
az ad user list --query "[?userType=='Guest']"
```

Ensure all users listed are still required and not inactive.

Audit from Azure PowerShell

```
Get-AzureADUser |Where-Object {$_.UserType -like "Guest"} |Select-Object
DisplayName, UserPrincipalName, UserType -Unique
```

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:** e9ac8f8e-ce22-4355-8f04-99b911d6be52 **- Name:** 'Guest accounts with read permissions on Azure resources should be removed'
- **Policy ID:** 94e1c2ac-cbbe-4cac-a2b5-389c812dee87 **- Name:** 'Guest accounts with write permissions on Azure resources should be removed'
- **Policy ID:** 339353f6-2387-4a45-abe4-7f529d121046 **- Name:** 'Guest accounts with owner permissions on Azure resources should be removed'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Click on `Add filter`
5. Select `User type`
6. Select `Guest` from the Value dropdown
7. Click `Apply`
8. Check the box next to all `Guest` users that are no longer required or are inactive
9. Click `Delete`
10. Click `OK`

Remediate from Azure CLI
Before deleting the user, set it to inactive using the ID from the Audit Procedure to determine if there are any dependent systems.

```
az ad user update --id <exampleaccountid@domain.com> --account-enabled
{false}
```

After determining that there are no dependent systems, delete the user.

```
Remove-AzureADUser -ObjectId <exampleaccountid@domain.com>
```

Remediate from Azure PowerShell
Before deleting the user, set it to inactive using the ID from the Audit Procedure to determine if there are any dependent systems.

```
Set-AzureADUser -ObjectId "<exampleaccountid@domain.com>" -AccountEnabled
false
```

After determining that there are no dependent systems, delete the user.

```
PS C:\>Remove-AzureADUser -ObjectId exampleaccountid@domain.com
```

Default Value:

By default no guest users are created.

References:

1. https://learn.microsoft.com/en-us/entra/external-id/user-properties
2. https://learn.microsoft.com/en-us/entra/fundamentals/how-to-create-delete-users#delete-a-user
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-4-review-and-reconcile-user-access-regularly
4. https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing
5. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-manage-inactive-user-accounts
6. https://learn.microsoft.com/en-us/entra/fundamentals/users-restore

Additional Information:

It is good practice to use a dynamic security group to manage guest users.

To create the dynamic security group:

1. Navigate to the 'Microsoft Entra ID' blade in the Azure Portal
2. Select the 'Groups' item
3. Create new
4. Type of 'dynamic'
5. Use the following dynamic selection rule. "(user.userType -eq "Guest")"
6. Once the group has been created, select access reviews option and create a new access review with a period of monthly and send to relevant administrators for review.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1018

6.3.3 Ensure that use of the 'User Access Administrator' role is restricted (Automated)

Profile Applicability:

- Level 1

Description:

The User Access Administrator role grants the ability to view all resources and manage access assignments at any subscription or management group level within the tenant. Due to its high privilege level, this role assignment should be removed immediately after completing the necessary changes at the root scope to minimize security risks.

Rationale:

The User Access Administrator role provides extensive access control privileges. Unnecessary assignments heighten the risk of privilege escalation and unauthorized access. Removing the role immediately after use minimizes security exposure.

Impact:

Increased administrative effort to manage and remove role assignments appropriately.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Subscriptions`.
3. Select a subscription.
4. Select `Access control (IAM)`.
5. Look for the following banner at the top of the page: `Action required: X users have elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access.` If the banner is displayed, the `User Access Administrator` is assigned.

Audit from Azure CLI

Run the following command:

```
az role assignment list --role "User Access Administrator" --scope "/"
```

Ensure that the command does not return any `User Access Administrator` role assignment information.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Subscriptions`.
3. Select a subscription.
4. Select `Access control (IAM)`.
5. Look for the following banner at the top of the page: `Action required: X users have elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access.`
6. Click `View role assignments`.
7. Click `Remove`.

Remediate from Azure CLI

Run the following command:

```
az role assignment delete --role "User Access Administrator" --scope "/"
```

References:

1. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
2. https://learn.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548	TA0004	M1018

6.3.4 Ensure that all 'privileged' role assignments are periodically reviewed (Manual)

Profile Applicability:

- Level 1

Description:

Periodic review of privileged role assignments is performed to ensure that the privileged roles assigned to users are accurate and appropriate.

Rationale:

Privileged roles are crown jewel assets that can be used by malicious insiders, threat actors, and even through mistake to significantly damage an organization in numerous ways. These roles should be periodically reviewed to:

- identify lingering permissions assignment (e.g. an administrator has been terminated, the administrator account is being retained, but the permissions are no longer necessary and has not been properly addressed by process)
- detect lateral movement through privilege escalation (e.g. an account with administrative permission has been compromised and is elevating other accounts in an attempt to circumvent detection mechanisms)

Impact:

Increased administrative effort to manage and remove role assignments appropriately.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Subscriptions`.
3. Select a subscription.
4. Select `Access control (IAM)`.
5. Look for the number under the word `Privileged` accompanied by a link titled `View Assignments.` Click the `View assignments` link.
6. For each privileged role listed, evaluate whether the assignment is appropriate and current for each User, Group, or App assigned to each privileged role.

NOTE: The judgement of what constitutes 'appropriate and current' assignments requires a clear understanding of your organization's personnel, systems, policy, and security requirements. This cannot be effectively prescribed in procedure.

Remediation:

References:

1. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1548	TA0004	M1018

6.4 Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1

Description:

Require administrators or appropriately delegated users to create new tenants.

Rationale:

It is recommended to only allow an administrator to create new tenants. This prevent users from creating new Microsoft Entra ID or Azure AD B2C tenants and ensures that only authorized users are able to do so.

Impact:

Enforcing this setting will ensure that only authorized users are able to create new tenants.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Ensure that `Restrict non-admin users from creating tenants` is set to `Yes`

Audit from PowerShell

```
Import-Module Microsoft.Graph.Identity.SignIns
Connect-MgGraph -Scopes 'Policy.ReadWrite.Authorization'
Get-MgPolicyAuthorizationPolicy | Select-Object -ExpandProperty
DefaultUserRolePermissions | Format-List
```

Review the "DefaultUserRolePermissions" section of the output. Ensure that `AllowedToCreateTenants` is not `"True"`.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Set `Restrict non-admin users from creating tenants` to `Yes`
6. Click `Save`

Remediate from PowerShell

```
Import-Module Microsoft.Graph.Identity.SignIns

Connect-MgGraph -Scopes 'Policy.ReadWrite.Authorization'

Select-MgProfile -Name beta

$params = @{
DefaultUserRolePermissions = @{
AllowedToCreateTenants = $false
}
}

Update-MgPolicyAuthorizationPolicy -AuthorizationPolicyId  -BodyParameter
$params
```

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions
2. https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#tenant-creator
3. https://blog.admindroid.com/disable-users-creating-new-azure-ad-tenants-in-microsoft-365/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

6.5 Ensure that 'Number of methods required to reset' is set to '2' (Manual)

Profile Applicability:

- Level 1

Description:

Ensures that two alternate forms of identification are provided before allowing a password reset.

Rationale:

A Self-service Password Reset (SSPR) through Azure Multi-factor Authentication (MFA) ensures the user's identity is confirmed using two separate methods of identification. With multiple methods set, an attacker would have to compromise both methods before they could maliciously reset a user's password.

Impact:

There may be administrative overhead, as users who lose access to their secondary authentication methods will need an administrator with permissions to remove it. There will also need to be organization-wide security policies and training to teach administrators to verify the identity of the requesting user so that social engineering cannot render this setting useless.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Select `Authentication methods`
6. Ensure that `Number of methods required to reset` is set to `2`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Select `Authentication methods`
6. Set the `Number of methods required to reset` to `2`
7. Click `Save`

Default Value:

By default, the `Number of methods required to reset` is set to "2".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls
4. https://learn.microsoft.com/en-us/entra/identity/authentication/passwords-faq#password-reset-registration
5. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
6. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1032

6.6 Ensure that account 'Lockout threshold' is less than or equal to '10' (Manual)

Profile Applicability:

- Level 1

Description:

The account lockout threshold determines how many failed login attempts are permitted prior to placing the account in a locked-out state and initiating a variable lockout duration.

Rationale:

Account lockout is a method of protecting against brute-force and password spray attacks. Once the lockout threshold has been exceeded, the account enters a locked-out state which prevents all login attempts for a variable duration. The lockout in combination with a reasonable duration reduces the total number of failed login attempts that a malicious actor can execute in a given period of time.

Impact:

If account lockout threshold is set too low (less than 3), users may experience frequent lockout events and the resulting security alerts may contribute to alert fatigue.

If account lockout threshold is set too high (more than 10), malicious actors can programmatically execute more password attempts in a given period of time.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Ensure that `Lockout threshold` is set to `10` or fewer.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Set the `Lockout threshold` to `10` or fewer.
7. Click `Save`.

Default Value:

By default, Lockout threshold is set to `10`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values

Additional Information:

NOTE: The variable number for failed login attempts allowed before lockout is prescribed by many security and compliance frameworks. The **appropriate** setting for this variable should be determined by the most restrictive security or compliance framework that your organization follows.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●

6.7 Ensure that account 'Lockout duration in seconds' is greater than or equal to '60' (Manual)

Profile Applicability:

- Level 1

Description:

The account lockout duration value determines how long an account retains the status of lockout, and therefore how long before a user can continue to attempt to login after passing the lockout threshold.

Rationale:

Account lockout is a method of protecting against brute-force and password spray attacks. Once the lockout threshold has been exceeded, the account enters a locked-out state which prevents all login attempts for a variable duration. The lockout in combination with a reasonable duration reduces the total number of failed login attempts that a malicious actor can execute in a given period of time.

Impact:

If account lockout duration is set too low (less than 60 seconds), malicious actors can perform more password spray and brute-force attempts over a given period of time.

If the account lockout duration is set too high (more than 300 seconds) users may experience inconvenient delays during lockout.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Ensure that `Lockout duration in seconds` is set to `60` or higher.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Set the `Lockout duration in seconds` to `60` or higher.
7. Click `Save`.

Default Value:

By default, Lockout duration in seconds is set to `60`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●

6.8 Ensure that a 'Custom banned password list' is set to 'Enforce' (Manual)

Profile Applicability:

- Level 1

Description:

Microsoft Azure applies a default global banned password list to all user and admin accounts that are created and managed directly in Microsoft Entra ID.

The Microsoft Entra password policy does not apply to user accounts that are synchronized from an on-premises Active Directory environment, unless Microsoft Entra ID Connect is used and `EnforceCloudPasswordPolicyForPasswordSyncedUsers` is enabled.

Review the `Default Value` section for more detail on the password policy.

For increased password security, a custom banned password list is recommended

Rationale:

Implementing a custom banned password list gives your organization further control over the password policy. Disallowing easy-to-guess passwords increases the security of your Azure resources.

Impact:

Increasing password complexity may increase user account administration overhead. Utilizing the default global banned password list and a custom list requires a Microsoft Entra ID P1 or P2 license. On-premises Active Directory Domain Services users who aren't synchronized to Microsoft Entra ID still benefit from Microsoft Entra ID Password Protection based on the existing licensing of synchronized users.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Ensure `Enforce custom list` is set to `Yes`.
7. Review the list of words banned from use in passwords.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Set the `Enforce custom list` option to `Yes`.
7. Click in the `Custom banned password list` text box.
8. Add a list of words, one per line, to prevent users from using in passwords.
9. Click `Save`.

Default Value:

By default the custom banned password list is not 'Enabled'. Organization-specific terms can be added to the custom banned password list, such as the following examples:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific terms
- Abbreviations that have specific company meaning
- Months and weekdays with your company's local languages

The default global banned password list is already applied to your resources which applies the following basic requirements:

Characters allowed:

- Uppercase characters (A - Z)
- Lowercase characters (a - z)
- Numbers (0 - 9)
- Symbols:
- @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < >
- blank space

Characters not allowed:

- Unicode characters

Password length:

Passwords require:

- A minimum of eight characters

- A maximum of 256 characters

Password complexity:

Passwords require three out of four of the following categories:

- Uppercase characters
- Lowercase characters
- Numbers
- Symbols

Note: Password complexity check isn't required for Education tenants.

Password not recently used:

- When a user changes or resets their password, the new password can't be the same as the current or recently used passwords.
- Password isn't banned by Entra ID Password Protection.
- The password can't be on the global list of banned passwords for Azure AD Password Protection, or on the customizable list of banned passwords specific to your organization.

Evaluation

New passwords are evaluated for strength and complexity by validating against the combined list of terms from the global and custom banned password lists. Even if a user's password contains a banned password, the password may be accepted if the overall password is otherwise strong enough.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-combined-policy
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad
3. https://docs.microsoft.com/en-us/powershell/module/Azuread/
4. https://www.microsoft.com/en-us/research/publication/password-guidance/
5. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1027

6.9 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the number of days before users are asked to re-confirm their authentication information is not set to 0.

Rationale:

This setting is necessary if 'Require users to register when signing in' is enabled. If authentication re-confirmation is disabled, registered users will never be prompted to re-confirm their existing authentication information. If the authentication information for a user changes, such as a phone number or email, then the password reset information for that user reverts to the previously registered authentication information.

Impact:

Users will be prompted to re-confirm their authentication information after the number of days specified.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Users`.
4. Select `Password reset`.
5. Under `Manage`, select `Registration`.
6. Ensure that `Number of days before users are asked to re-confirm their authentication information` is not set to `0`.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Users`.
4. Select `Password reset`.
5. Under `Manage`, select `Registration`.
6. Set the `Number of days before users are asked to re-confirm their authentication information` to your organization-defined frequency.
7. Click `Save`.

Default Value:

By default, the `Number of days before users are asked to re-confirm their authentication information` is set to "180 days".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#registration
2. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

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	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1027

6.10 Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that users are notified on their primary and alternate emails on password resets.

Rationale:

User notification on password reset is a proactive way of confirming password reset activity. It helps the user to recognize unauthorized password reset activities.

Impact:

Users will receive emails alerting them to password changes to both their primary and alternate emails.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage`, select `Notifications`
6. Ensure that `Notify users on password resets?` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage`, select `Notifications`
6. Set `Notify users on password resets?` to `Yes`
7. Click `Save`

Default Value:

By default, `Notify users on password resets?` is set to "Yes".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#set-up-notifications-and-customizations
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#notifications
3. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1027

6.11 Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that all Global Administrators are notified if any other administrator resets their password.

Rationale:

Administrator accounts are sensitive. Any password reset activity notification, when sent to all Administrators, ensures that all Global Administrators can passively confirm if such a reset is a common pattern within their group. For example, if all Administrators change their password every 30 days, any password reset activity before that may require administrator(s) to evaluate any unusual activity and confirm its origin.

Impact:

All Global Administrators will receive a notification from Azure every time a password is reset. This is useful for auditing procedures to confirm that there are no out of the ordinary password resets for Administrators. There is additional overhead, however, in the time required for Global Administrators to audit the notifications. This setting is only useful if all Global Administrators pay attention to the notifications and audit each one.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage`, select `Notifications`
6. Ensure that `Notify all admins when other admins reset their password?` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage`, select `Notifications`
6. Set `Notify all admins when other admins reset their password?` to `Yes`

7. Click `Save`

Default Value:

By default, `Notify all admins when other admins reset their password?` is set to "No".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#notifications
2. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#set-up-notifications-and-customizations

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1026

6.12 Ensure that 'User consent for applications' is set to 'Do not allow user consent' (Manual)

Profile Applicability:

- Level 1

Description:

Require administrators to provide consent for applications before use.

Rationale:

If Microsoft Entra ID is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts.

Impact:

Enforcing this setting may create additional requests that administrators need to review.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Enterprise applications`
4. Under `Security`, select `Consent and permissions`
5. Under `Manage`, select `User consent settings`
6. Ensure `User consent for applications` is set to `Do not allow user consent`

Audit from PowerShell

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Select-Object
-ExpandProperty PermissionGrantPoliciesAssigned
```

If the command returns no values in response, the configuration complies with the recommendation.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Enterprise applications`
4. Under `Security`, select `Consent and permissions`
5. Under `Manage`, select `User consent settings`
6. Set `User consent for applications` to `Do not allow user consent`
7. Click `Save`

Default Value:

By default, `Users consent for applications` is set to `Allow user consent for apps`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=ms-powershell#configure-user-consent-to-applications
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

6.13 Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions' (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to provide consent for selected permissions when a request is coming from a verified publisher.

Rationale:

If Microsoft Entra ID is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts.

Impact:

Enforcing this setting may create additional requests that administrators need to review.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Enterprise applications`
4. Under `Security, select` Consent and permissions`
5. Under `Manage`, select `User consent settings`
6. Under `User consent for applications`, ensure `Allow user consent for apps from verified publishers, for selected permissions` is selected

Audit from PowerShell

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Select-Object
-ExpandProperty PermissionGrantPoliciesAssigned
```

The command should return either `ManagePermissionGrantsForSelf.microsoft-user-default-low` or a custom app consent policy id if one is in use.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`

3. Under `Manage`, select `Enterprise applications`
4. Under `Security, select` Consent and permissions`
5. Under `Manage`, select `User consent settings`
6. Under `User consent for applications`, select `Allow user consent for apps from verified publishers, for selected permissions`
7. Click `Save`

Default Value:

By default, `User consent for applications` is set to `Allow user consent for apps`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=ms-graph#configure-user-consent-to-applications
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
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/powershell/module/microsoft.graph.identity.signins/get-mgpolicyauthorizationpolicy?view=graph-powershell-1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

6.14 Ensure that 'Users can register applications' is set to 'No' (Automated)

Profile Applicability:

- Level 1

Description:

Require administrators or appropriately delegated users to register third-party applications.

Rationale:

It is recommended to only allow an administrator to register custom-developed applications. This ensures that the application undergoes a formal security review and approval process prior to exposing Microsoft Entra ID data. Certain users like developers or other high-request users may also be delegated permissions to prevent them from waiting on an administrative user. Your organization should review your policies and decide your needs.

Impact:

Enforcing this setting will create additional requests for approval that will need to be addressed by an administrator. If permissions are delegated, a user may approve a malevolent third party application, potentially giving it access to your data.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Ensure that `Users can register applications` is set to `No`

Audit from PowerShell

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Format-List
AllowedToCreateApps
```

Command should return the value of `False`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`

3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Set `Users can register applications` to `No`
6. Click `Save`

Remediate from PowerShell

```
$param = @{ AllowedToCreateApps = "$false" }
Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $param
```

Default Value:

By default, `Users can register applications` is set to "Yes".

References:

1. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#restrict-who-can-create-applications
2. https://learn.microsoft.com/en-us/entra/identity-platform/how-applications-are-added#who-has-permission-to-add-applications-to-my-azure-ad-instance
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/get-mgpolicyauthorizationpolicy?view=graph-powershell-1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	2.4 Utilize Automated Software Inventory Tools Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

6.15 Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Automated)

Profile Applicability:

- Level 1

Description:

Limit guest user permissions.

Rationale:

Limiting guest access ensures that guest accounts do not have permission for certain directory tasks, such as enumerating users, groups or other directory resources, and cannot be assigned to administrative roles in your directory. Guest access has three levels of restriction.

1. Guest users have the same access as members (most inclusive),
2. Guest users have limited access to properties and memberships of directory objects (default value),
3. Guest user access is restricted to properties and memberships of their own directory objects (most restrictive).

The recommended option is the 3rd, most restrictive: "Guest user access is restricted to their own directory object".

Impact:

This may create additional requests for permissions to access resources that administrators will need to approve.

According to https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions#services-currently-not-supported

Service without current support might have compatibility issues with the new guest restriction setting.

- Forms
- Project
- Yammer
- Planner in SharePoint

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest user access`, ensure that `Guest user access restrictions` is set to `Guest user access is restricted to properties and memberships of their own directory objects`

Audit from PowerShell

1. Enter the following:

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).GuestUserRoleId
```

Which will give a result like:

```
Id                                                 : authorizationPolicy
OdataType                                          :
Description                                        : Used to manage
authorization related settings across the company.
DisplayName                                        : Authorization Policy
EnabledPreviewFeatures                             : {}
GuestUserRoleId                                    : 10dae51f-b6af-4016-8d66-
8c2a99b929b3
PermissionGrantPolicyIdsAssignedToDefaultUserRole : {user-default-legacy}
```

If the GuestUserRoleID property does not equal `2af84b1e-32c8-42b7-82bc-daa82404023b` then it is not set to most restrictive.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest user access`, set `Guest user access restrictions` to `Guest user access is restricted to properties and memberships of their own directory objects`
6. Click `Save`

Remediate from PowerShell

1. Enter the following to update the policy ID:

```
Update-MgPolicyAuthorizationPolicy -GuestUserRoleId "2af84b1e-32c8-42b7-82bc-daa82404023b"
```

1. Check the GuestUserRoleId again:

```
(Get-MgPolicyAuthorizationPolicy).GuestUserRoleId
```

1. Ensure that the GuestUserRoleId is equal to the earlier entered value of `2af84b1e-32c8-42b7-82bc-daa82404023b`.

Default Value:

By default, `Guest user access restrictions` is set to `Guest users have limited access to properties and memberships of directory objects`.

References:

1. https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions#member-and-guest-users
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
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/entra/identity/users/users-restrict-guest-permissions

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1026

6.16 Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' (Automated)

Profile Applicability:

- Level 2

Description:

Restrict invitations to users with specific administrative roles only.

Rationale:

Restricting invitations to users with specific administrator roles ensures that only authorized accounts have access to cloud resources. This helps to maintain "Need to Know" permissions and prevents inadvertent access to data.

By default the setting `Guest invite restrictions` is set to `Anyone in the organization can invite guest users including guests and non-admins`. This would allow anyone within the organization to invite guests and non-admins to the tenant, posing a security risk.

Impact:

With the option of `Only users assigned to specific admin roles can invite guest users` selected, users with specific admin roles will be in charge of sending invitations to the external users, requiring additional overhead by them to manage user accounts. This will mean coordinating with other departments as they are onboarding new users.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest invite settings`, for `Guest invite restrictions`, ensure that `Only users assigned to specific admin roles can invite guest users` is selected

Note: This setting has 4 levels of restriction, which include:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive),

- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions,
- Only users assigned to specific admin roles can invite guest users,
- No one in the organization can invite guest users including admins (most restrictive).

Audit from Powershell

Enter the following:

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).AllowInvitesFrom
```

If the resulting value is `adminsAndGuestInviters` the configuration complies.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest invite settings`, set `Guest invite restrictions`, to `Only users assigned to specific admin roles can invite guest users`
6. Click `Save`

Remediate from Powershell

Enter the following:

```
Connect-MgGraph
Update-MgPolicyAuthorizationPolicy -AllowInvitesFrom "adminsAndGuestInviters"
```

Default Value:

By default, `Guest invite restrictions` is set to `Anyone in the organization can invite guest users including guests and non-admins`

References:

1. https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements

5. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/update-mgpolicyauthorizationpolicy?view=graph-powershell-1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1026

6.17 Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Restrict access to the Microsoft Entra ID administration center to administrators only.

NOTE: This only affects access to the Entra ID administrator's web portal. This setting does not prohibit privileged users from using other methods such as Rest API or Powershell to obtain sensitive information from Microsoft Entra ID.

Rationale:

The Microsoft Entra ID administrative center has sensitive data and permission settings. All non-administrators should be prohibited from accessing any Microsoft Entra ID data in the administration center to avoid exposure.

Impact:

All administrative tasks will need to be done by Administrators, causing additional overhead in management of users and resources.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Under `Administration centre`, ensure that `Restrict access to Microsoft Entra admin center` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Under `Administration centre`, set `Restrict access to Microsoft Entra admin center` to `Yes`
6. Click `Save`

Default Value:

By default, `Restrict access to Microsoft Entra admin center` is set to `No`

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles-azure-portal
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-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1538	TA0007	M1018

6.18 Ensure that 'Restrict user ability to access groups features in My Groups' is set to 'Yes' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict access to group web interface in the Access Panel portal.

Rationale:

Self-service group management enables users to create and manage security groups or Office 365 groups in Microsoft Entra ID. Unless a business requires this day-to-day delegation for some users, self-service group management should be disabled. Any user can access the Access Panel, where they can reset their passwords, view their information, etc. By default, users are also allowed to access the Group feature, which shows groups, members, related resources (SharePoint URL, Group email address, Yammer URL, and Teams URL). By setting this feature to 'Yes', users will no longer have access to the web interface, but still have access to the data using the API. This is useful to prevent non-technical users from enumerating groups-related information, but technical users will still be able to access this information using APIs.

Impact:

Setting to `Yes` could create administrative overhead by customers seeking certain group memberships that will have to be manually managed by administrators with appropriate permissions.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Self Service Group Management`, ensure that `Restrict user ability to access groups features in My Groups` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Self Service Group Management`, set `Restrict user ability to access groups features in My Groups` to `Yes`
6. Click `Save`

Default Value:

By default, `Restrict user ability to access groups features in the Access Pane` is set to `No`

References:

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

6.19 Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict security group creation to administrators only.

Rationale:

When creating security groups is enabled, all users in the directory are allowed to create new security groups and add members to those groups. Unless a business requires this day-to-day delegation, security group creation should be restricted to administrators only.

Impact:

Enabling this setting could create a number of requests that would need to be managed by an administrator.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Security Groups`, ensure that `Users can create security groups in Azure portals, API or PowerShell` is set to `No`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Security Groups`, set `Users can create security groups in Azure portals, API or PowerShell` to `No`
6. Click `Save`

Default Value:

By default, `Users can create security groups in Azure portals, API or PowerShell` is set to `Yes`

References:

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management#making-a-group-available-for-end-user-self-service
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1578	TA0005	M1018

6.20 Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict security group management to administrators only.

Rationale:

Restricting security group management to administrators only prohibits users from making changes to security groups. This ensures that security groups are appropriately managed and their management is not delegated to non-administrators.

Impact:

Group Membership for user accounts will need to be handled by Admins and cause administrative overhead.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Self Service Group Management`, ensure that `Owners can manage group membership requests in My Groups` is set to `No`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Self Service Group Management`, set `Owners can manage group membership requests in My Groups` to `No`
6. Click `Save`

Default Value:

By default, `Owners can manage group membership requests in My Groups` is set to `No`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management#making-a-group-available-for-end-user-self-service
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-8-determine-access-process-for-cloud-provider-support
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

6.21 Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict Microsoft 365 group creation to administrators only.

Rationale:

Restricting Microsoft 365 group creation to administrators only ensures that creation of Microsoft 365 groups is controlled by the administrator. Appropriate groups should be created and managed by the administrator and group creation rights should not be delegated to any other user.

Impact:

Enabling this setting could create a number of requests that would need to be managed by an administrator.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Microsoft 365 Groups`, ensure that `Users can create Microsoft 365 groups in Azure portals, API or PowerShell` is set to `No`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Microsoft 365 Groups`, set `Users can create Microsoft 365 groups in Azure portals, API or PowerShell` to `No`
6. Click `Save`

Default Value:

By default, `Users can create Microsoft 365 groups in Azure portals, API or PowerShell` is set to `Yes`.

References:

1. https://learn.microsoft.com/en-us/microsoft-365/solutions/manage-creation-of-groups?view=o365-worldwide&redirectSourcePath=%252fen-us%252farticle%252fControl-who-can-create-Office-365-Groups-4c46c8cb-17d0-44b5-9776-005fced8e618
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1578	TA0005	M1018

6.22 Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

NOTE: This recommendation is only relevant if your subscription is using Per-User MFA. If your organization is licensed to use Conditional Access, the preferred method of requiring MFA to join devices to Entra ID is to use a Conditional Access policy (see additional information below for link).

Joining or registering devices to Microsoft Entra ID should require multi-factor authentication.

Rationale:

Multi-factor authentication is recommended when adding devices to Microsoft Entra ID. When set to `Yes`, users who are adding devices from the internet must first use the second method of authentication before their device is successfully added to the directory. This ensures that rogue devices are not added to the domain using a compromised user account.

Impact:

A slight impact of additional overhead, as Administrators will now have to approve every access to the domain.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Devices`
4. Under `Manage`, select `Device settings`
5. Under `Microsoft Entra join and registration settings`, ensure that `Require Multifactor Authentication to register or join devices with Microsoft Entra` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Devices`
4. Under `Manage`, select `Device settings`

5. Under `Microsoft Entra join and registration settings`, set `Require Multifactor Authentication to register or join devices with Microsoft Entra` to `Yes`
6. Click `Save`

Default Value:

By default, `Require Multifactor Authentication to register or join devices with Microsoft Entra` is set to `No`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-mfa-device-register-join
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls

Additional Information:

If Conditional Access is available, this recommendation should be bypassed in favor of the Conditional Access implementation of requiring Multifactor Authentication to register or join devices with Microsoft Entra.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-mfa-device-register-join

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1078.004	TA0001	M1032

6.23 Ensure that no custom subscription administrator roles exist (Automated)

Profile Applicability:

- Level 1

Description:

The principle of least privilege should be followed and only necessary privileges should be assigned instead of allowing full administrative access.

Rationale:

Custom roles in Azure with administrative access can obfuscate the permissions granted and introduce complexity and blind spots to the management of privileged identities. For less mature security programs without regular identity audits, the creation of Custom roles should be avoided entirely. For more mature security programs with regular identity audits, Custom Roles should be audited for use and assignment, used minimally, and the principle of least privilege should be observed when granting permissions

Impact:

Subscriptions will need to be handled by Administrators with permissions.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Subscriptions`.
3. Select a subscription.
4. Select `Access control (IAM)`.
5. Select `Roles`.
6. Click `Type` and select `Custom role` from the drop-down menu.
7. Select `View` next to a role.
8. Select `JSON`.
9. Check for `assignableScopes` set to the subscription, and `actions` set to `*`.
10. Repeat steps 7-9 for each custom role.

Audit from Azure CLI
List custom roles:

```
az role definition list --custom-role-only True
```

Check for entries with `assignableScope` of the `subscription`, and an action of `*`

Audit from PowerShell

```
Connect-AzAccount
Get-AzRoleDefinition |Where-Object {($_.IsCustom -eq $true) -and
($_.Actions.contains('*'))}
```

Check the output for `AssignableScopes` value set to the subscription.

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:** a451c1ef-c6ca-483d-87ed-f49761e3ffb5 **- Name:** 'Audit usage of custom RBAC roles'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Subscriptions`.
3. Select a subscription.
4. Select `Access control (IAM)`.
5. Select `Roles`.
6. Click `Type` and select `Custom role` from the drop-down menu.
7. Check the box next to each role which grants subscription administrator privileges.
8. Select `Delete`.
9. Select `Yes`.

Remediate from Azure CLI

List custom roles:

```
az role definition list --custom-role-only True
```

Check for entries with `assignableScope` of the `subscription`, and an action of `*`.
To remove a violating role:

```
az role definition delete --name <role name>
```

Note that any role assignments must be removed before a custom role can be deleted. Ensure impact is assessed before deleting a custom role granting subscription administrator privileges.

Default Value:

By default, no custom owner roles are created.

References:

1. https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098.003	TA0003	M1026

6.24 Ensure that a custom role is assigned permissions for administering resource locks (Manual)

Profile Applicability:

- Level 2

Description:

Resource locking is a powerful protection mechanism that can prevent inadvertent modification or deletion of resources within Azure subscriptions and resource groups, and it is a recommended NIST configuration.

Rationale:

Given that the resource lock functionality is outside of standard Role-Based Access Control (RBAC), it would be prudent to create a resource lock administrator role to prevent inadvertent unlocking of resources.

Impact:

By adding this role, specific permissions may be granted for managing only resource locks rather than needing to provide the broad Owner or User Access Administrator role, reducing the risk of the user being able to cause unintentional damage.

Audit:

Audit from Azure Portal

1. In the Azure portal, navigate to a subscription or resource group.
2. Click `Access control (IAM)`.
3. Click `Roles`.
4. Click `Type : All`.
5. Click to view the drop-down menu.
6. Select `Custom role`.
7. Click `View` in the `Details` column of a custom role.
8. Review the role permissions.
9. Click `Assignments` and review the assignments.
10. Click the `X` to exit the custom role details page.
11. Repeat steps 7-10. Ensure that at least one custom role exists that assigns the `Microsoft.Authorization/locks` permission to appropriate members.
12. Repeat steps 1-11 for each subscription or resource group.

Remediation:

Remediate from Azure Portal

1. In the Azure portal, navigate to a subscription or resource group.
2. Click `Access control (IAM)`.
3. Click `+ Add`.
4. Click `Add custom role`.
5. In the `Custom role name` field enter `Resource Lock Administrator`.
6. In the `Description` field enter `Can Administer Resource Locks`.
7. For `Baseline permissions` select `Start from scratch`.
8. Click `Next`.
9. Click `Add permissions`.
10. In the `Search for a permission` box, type `Microsoft.Authorization/locks`.
11. Click the result.
12. Check the box next to `Permission`.
13. Click `Add`.
14. Click `Review + create`.
15. Click `Create`.
16. Click `OK`.
17. Click `+ Add`.
18. Click `Add role assignment`.
19. In the `Search by role name, description, permission, or ID` box, type `Resource Lock Administrator`.
20. Select the role.
21. Click `Next`.
22. Click `+ Select members`.
23. Select appropriate members.
24. Click `Select`.
25. Click `Review + assign`.
26. Click `Review + assign` again.
27. Repeat steps 1-26 for each subscription or resource group requiring remediation.

Remediate from PowerShell:
Below is a PowerShell definition for a resource lock administrator role created at an Azure Management group level

```
Import-Module Az.Accounts
Connect-AzAccount

$role = Get-AzRoleDefinition "User Access Administrator"
$role.Id = $null
$role.Name = "Resource Lock Administrator"
$role.Description = "Can Administer Resource Locks"
$role.Actions.Clear()
$role.Actions.Add("Microsoft.Authorization/locks/*")
$role.AssignableScopes.Clear()

* Scope at the Management group level Management group

$role.AssignableScopes.Add("/providers/Microsoft.Management/managementGroups/
MG-Name")

New-AzRoleDefinition -Role $role
Get-AzureRmRoleDefinition "Resource Lock Administrator"
```

Default Value:

A role for administering resource locks does not exist by default.

References:

1. https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
2. https://docs.microsoft.com/en-us/azure/role-based-access-control/check-access
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

6.25 Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one' (Manual)

Profile Applicability:

- Level 2

Description:

Users who are set as subscription owners are able to make administrative changes to the subscriptions and move them into and out of Microsoft Entra ID.

Rationale:

Permissions to move subscriptions in and out of a Microsoft Entra tenant must only be given to appropriate administrative personnel. A subscription that is moved into a Microsoft Entra tenant may be within a folder to which other users have elevated permissions. This prevents loss of data or unapproved changes of the objects within by potential bad actors.

Impact:

Subscriptions will need to have these settings turned off to be moved.

Audit:

Audit from Azure Portal

1. From the Azure Portal Home select the portal menu
2. Select `Subscriptions`
3. In the `Advanced options` drop-down menu, select `Manage Policies`
4. Ensure `Subscription leaving Microsoft Entra tenant` and `Subscription entering Microsoft Entra tenant` are set to `Permit no one`

Remediation:

Remediate from Azure Portal

1. From the Azure Portal Home select the portal menu
2. Select `Subscriptions`
3. In the `Advanced options` drop-down menu, select `Manage Policies`
4. Set `Subscription leaving Microsoft Entra tenant` and `Subscription entering Microsoft Entra tenant` to `Permit no one`
5. Click `Save changes`

Default Value:

By default `Subscription leaving Microsoft Entra tenant` and `Subscription entering Microsoft Entra tenant` are set to `Allow everyone (default)`

References:

1. https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/manage-azure-subscription-policy
2. https://learn.microsoft.com/en-us/entra/fundamentals/how-subscriptions-associated-directory
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-2-protect-identity-and-authentication-systems

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
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	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1578	TA0040	M1018

6.26 Ensure fewer than 5 users have global administrator assignment (Manual)

Profile Applicability:

- Level 1

Description:

This recommendation aims to maintain a balance between security and operational efficiency by ensuring that a minimum of 2 and a maximum of 4 users are assigned the Global Administrator role in Microsoft Entra ID. Having at least two Global Administrators ensures redundancy, while limiting the number to four reduces the risk of excessive privileged access.

Rationale:

The Global Administrator role has extensive privileges across all services in Microsoft Entra ID. The Global Administrator role should never be used in regular daily activities; administrators should have a regular user account for daily activities, and a separate account for administrative responsibilities. Limiting the number of Global Administrators helps mitigate the risk of unauthorized access, reduces the potential impact of human error, and aligns with the principle of least privilege to reduce the attack surface of an Azure tenant. Conversely, having at least two Global Administrators ensures that administrative functions can be performed without interruption in case of unavailability of a single admin.

Impact:

Implementing this recommendation may require changes in administrative workflows or the redistribution of roles and responsibilities. Adequate training and awareness should be provided to all Global Administrators.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Roles and administrators`
4. Under `Administrative Roles`, select `Global Administrator`
5. Ensure less than 5 users are actively assigned the role.
6. Ensure that at least 2 users are actively assigned the role.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Roles and administrators`
4. Under `Administrative Roles`, select `Global Administrator`

If more than 4 users are assigned:

1. Remove Global Administrator role for users which do not or no longer require the role.
2. Assign Global Administrator role via PIM which can be activated when required.
3. Assign more granular roles to users to conduct their duties.

If only one user is assigned:

1. Provide the Global Administrator role to a trusted user or create a break glass admin account.

References:

1. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices#5-limit-the-number-of-global-administrators-to-less-than-5
2. https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#security-guidelines-for-assigning-roles
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

7 Management and Governance Services

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#management-and-governance

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

7.1 Logging and Monitoring

This section covers security recommendations to follow for logging and monitoring policies on an Azure Subscription.

Scoping: A necessary exercise for effective and efficient use of Logging and Monitoring

For recommendations contained in this section, it is crucial that your organization consider and settle on the scope of application for each recommendation individually. The scope of application cannot be realistically written in a generic prescriptive way within these recommendations, so a scoping exercise is strongly recommended. A scoping exercise will help you determine which resources are "in scope" and will receive partial or complete logging and monitoring treatment, and which resources are "out of scope" and will not receive any logging and monitoring treatment.

Your objectives with the scoping exercise should be to:

- Produce a clear classification of resources
- Understand the control requirements of any relevant security or compliance frameworks
- Ensure the appropriate personnel can detect and react to threats
- Ensure relevant resources have a historical register for accountability and investigation
- Minimize alert fatigue and cost

Release Environments provide a helpful context for understanding scope from a DevOps perspective. For example:

1. Production Environment
2. Staging Environment
3. Testing Environment
4. Development Environment

While resources considered in the scope of a Production Environment might have a full set of recommendations applied for logging and monitoring, other release environments might have a limited set of recommendations applied for the sake of accountability. The names of these environments and which resources are in the scope of each environment will vary from one organization to another.

7.1.1 Configuring Diagnostic Settings

The Azure Diagnostic Settings capture control/management activities performed on a subscription or Azure AD Tenant. By default, the Azure Portal retains activity logs only for 90 days. The Diagnostic Settings define the type of events that are stored or streamed and the outputs—storage account, log analytics workspace, event hub, and others. The Diagnostic Settings, if configured properly, can ensure that all logs are retained for longer duration. This section has recommendations for correctly configuring the Diagnostic Settings so that all logs captured are retained for longer periods.

Azure Subscriptions

When configuring Diagnostic Settings, you may choose to export in one of four ways in which you need to ensure appropriate data retention. The options are Log Analytics workspace, Event Hub, Storage Account, and Partner Solutions. It is important to ensure you are aware and have set retention as your organization sees fit.

Azure AD Logs

In order to retain sign in logs, user account changes, application provisioning logs, or other logs that are visible to only on the Tenant in Azure AD, separate Diagnostic settings must be specified.

Deployment by Policy

Deploying Azure diagnostics should ideally be done by policy to ensure a consistent configuration. Microsoft provides a full set of policies for all diagnostic capable resource types in their GitHub repository. If you chose to deploy by policy, it is best to route the diagnostics to a Log Analytics Workspace so that they can be used in Azure Monitor or Azure Sentinel. Be aware that this has a cost attached to it. Future versions of the CIS Azure Foundations Benchmark will aim to cover the use of policy in greater detail.

7.1.1.1 Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs (Manual)

Profile Applicability:

- Level 1

Description:

Enable Diagnostic settings for exporting activity logs. Diagnostic settings are available for each individual resource within a subscription. Settings should be configured for all appropriate resources for your environment.

Rationale:

A diagnostic setting controls how a diagnostic log is exported. By default, logs are retained only for 90 days. Diagnostic settings should be defined so that logs can be exported and stored for a longer duration to analyze security activities within an Azure subscription.

Audit:

Audit from Azure Portal
To identify Diagnostic Settings on a subscription:

1. Go to `Monitor`
2. Click `Activity Log`
3. Click `Export Activity Logs`
4. Select a `Subscription`
5. Ensure a `Diagnostic setting` exists for the selected Subscription

To identify Diagnostic Settings on specific resources:

1. Go to `Monitoring`
2. Click `Diagnostic settings`
3. Ensure a `Diagnostic setting` exists for all appropriate resources.

Audit from Azure CLI
To identify Diagnostic Settings on a subscription:

```
az monitor diagnostic-settings subscription list --subscription <subscription ID>
```

To identify Diagnostic Settings on a resource

```
az monitor diagnostic-settings list --resource <resource Id>
```

Audit from PowerShell
To identify Diagnostic Settings on a Subscription:

```
Get-AzDiagnosticSetting -SubscriptionId <subscription ID>
```

To identify Diagnostic Settings on a specific resource:

```
Get-AzDiagnosticSetting -ResourceId <resource ID>
```

Remediation:

Remediate from Azure Portal
To enable Diagnostic Settings on a Subscription:

1. Go to `Monitor`
2. Click on `Activity log`
3. Click on `Export Activity Logs`
4. Click `+ Add diagnostic setting`
5. Enter a `Diagnostic setting name`
6. Select `Categories` for the diagnostic setting
7. Select the appropriate `Destination details` (this may be Log Analytics, Storage Account, Event Hub, or Partner solution)
8. Click `Save`

To enable Diagnostic Settings on a specific resource:

1. Go to `Monitoring`
2. Click `Diagnostic settings`
3. Select `Add diagnostic setting`
4. Enter a `Diagnostic setting name`
5. Select the appropriate log, metric, and destination (this may be Log Analytics, Storage Account, Event Hub, or Partner solution)
6. Click `Save`

Repeat these step for all resources as needed.
Remediate from Azure CLI
To configure Diagnostic Settings on a Subscription:

```
az monitor diagnostic-settings subscription create --subscription
<subscription id> --name <diagnostic settings name> --location <location> <[-
-event-hub <event hub ID> --event-hub-auth-rule <event hub auth rule ID>] [--
storage-account <storage account ID>] [--workspace <log analytics workspace
ID>] --logs "<JSON encoded categories>" (e.g.
[{category:Security,enabled:true},{category:Administrative,enabled:true},{cat
egory:Alert,enabled:true},{category:Policy,enabled:true}])
```

To configure Diagnostic Settings on a specific resource:

```
az monitor diagnostic-settings create --subscription <subscription ID> --
resource <resource ID> --name <diagnostic settings name> <[--event-hub <event
hub ID> --event-hub-rule <event hub auth rule ID>] [--storage-account
<storage account ID>] [--workspace <log analytics workspace ID>] --logs
<resource specific JSON encoded log settings> --metrics <metric settings
(shorthand|json-file|yaml-file)>
```

Remediate from PowerShell

To configure Diagnostic Settings on a subscription:

```
$logCategories = @();
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Administrative -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Security -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category ServiceHealth -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Alert -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Recommendation -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Policy -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Autoscale -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category ResourceHealth -Enabled $true

New-AzSubscriptionDiagnosticSetting -SubscriptionId <subscription ID> -Name
<Diagnostic settings name> <[-EventHubAuthorizationRule <event hub auth rule
ID> -EventHubName <event hub name>] [-StorageAccountId <storage account ID>]
[-WorkSpaceId <log analytics workspace ID>] [-MarketplacePartner ID <full ARM
Marketplace resource ID>]> -Log $logCategories
```

To configure Diagnostic Settings on a specific resource:

```
$logCategories = @()
$logCategories +=  New-AzDiagnosticSettingLogSettingsObject -Category
<resource specific log category> -Enabled $true

Repeat command and variable assignment for each Log category specific to the
resource where this Diagnostic Setting will get configured.


$metricCategories = @()
$metricCategories += New-AzDiagnosticSettingMetricSettingsObject -Enabled
$true [-Category <resource specific metric category | AllMetrics>] [-
RetentionPolicyDay <Integer>] [-RetentionPolicyEnabled $true]

Repeat command and variable assignment for each Metric category or use the
'AllMetrics' category.


New-AzDiagnosticSetting -ResourceId <resource ID> -Name <Diagnostic settings
name> -Log $logCategories -Metric $metricCategories [-
EventHubAuthorizationRuleId <event hub auth rule ID> -EventHubName <event hub
name>] [-StorageAccountId <storage account ID>] [-WorkspaceId <log analytics
workspace ID>] [-MarketplacePartnerId <full ARM marketplace resource ID>]>
```

Default Value:

By default, diagnostic setting is not set.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs#export-the-activity-log-with-a-log-profile
2. https://learn.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

7.1.1.2 Ensure Diagnostic Setting captures appropriate categories (Automated)

Profile Applicability:

- Level 1

Description:

Prerequisite: A Diagnostic Setting must exist. If a Diagnostic Setting does not exist, the navigation and options within this recommendation will not be available. Please review the recommendation at the beginning of this subsection titled: "Ensure that a 'Diagnostic Setting' exists."

The diagnostic setting should be configured to log the appropriate activities from the control/management plane.

Rationale:

A diagnostic setting controls how the diagnostic log is exported. Capturing the diagnostic setting categories for appropriate control/management plane activities allows proper alerting.

Audit:

Audit from Azure Portal

1. Go to `Monitor`.
2. Click `Activity log`.
3. Click on `Export Activity Logs`.
4. Select the appropriate `Subscription`.
5. Click `Edit setting` next to a diagnostic setting.
6. Ensure that the following categories are checked: `Administrative, Alert, Policy, and Security`.

Audit from Azure CLI
Ensure the categories `'Administrative', 'Alert', 'Policy', and 'Security'` set to: 'enabled: true'

```
az monitor diagnostic-settings subscription list --subscription <subscription ID>
```

Audit from PowerShell
Ensure the categories Administrative, Alert, Policy, and Security are set to Enabled:True

```
Get-AzSubscriptionDiagnosticSetting -Subscription <subscriptionID>
```

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:** 3b980d31-7904-4bb7-8575-5665739a8052 **- Name:** 'An activity log alert should exist for specific Security operations'
- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'
- **Policy ID:** c5447c04-a4d7-4ba8-a263-c9ee321a6858 **- Name:** 'An activity log alert should exist for specific Policy operations'

Remediation:

Remediate from Azure Portal

1. Go to `Monitor`.
2. Click `Activity log`.
3. Click on `Export Activity Logs`.
4. Select the `Subscription` from the drop down menu.
5. Click `Edit setting` next to a diagnostic setting.
6. Check the following categories: `Administrative, Alert, Policy, and Security`.
7. Choose the destination details according to your organization's needs.
8. Click `Save`.

Remediate from Azure CLI

```
az monitor diagnostic-settings subscription create --subscription
<subscription id> --name <diagnostic settings name> --location <location> <[-
-event-hub <event hub ID> --event-hub-auth-rule <event hub auth rule ID>] [--
storage-account <storage account ID>] [--workspace <log analytics workspace
ID>] --logs
"[{category:Security,enabled:true},{category:Administrative,enabled:true},{ca
tegory:Alert,enabled:true},{category:Policy,enabled:true}]"
```

Remediate from PowerShell

```
$logCategories = @();
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Administrative -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Security -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Alert -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Policy -Enabled $true

New-AzSubscriptionDiagnosticSetting -SubscriptionId <subscription ID> -Name
<Diagnostic settings name> <[-EventHubAuthorizationRule <event hub auth rule
ID> -EventHubName <event hub name>] [-StorageAccountId <storage account ID>]
[-WorkSpaceId <log analytics workspace ID>] [-MarketplacePartner ID <full ARM
Marketplace resource ID>]> -Log $logCategories
```

Default Value:

When the diagnostic setting is created using Azure Portal, by default no categories are selected.

References:

1. https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings
2. https://docs.microsoft.com/en-us/azure/azure-monitor/samples/resource-manager-diagnostic-settings
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
4. https://learn.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest
5. https://learn.microsoft.com/en-us/powershell/module/az.monitor/new-azsubscriptiondiagnosticsetting?view=azps-9.2.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

7.1.1.3 Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Storage accounts with the activity log exports can be configured to use Customer Managed Keys (CMK).

Rationale:

Configuring the storage account with the activity log export container to use CMKs provides additional confidentiality controls on log data, as a given user must have read permission on the corresponding storage account and must be granted decrypt permission by the CMK.

Impact:

NOTE: You must have your key vault setup to utilize this. All Audit Logs will be encrypted with a key you provide. You will need to set up customer managed keys separately, and you will select which key to use via the instructions here. You will be responsible for the lifecycle of the keys, and will need to manually replace them at your own determined intervals to keep the data secure.

Audit:

Audit from Azure Portal

1. Go to `Monitor`.
2. Select `Activity log`.
3. Select `Export Activity Logs`.
4. Select a `Subscription`.
5. Note the name of the `Storage Account` for the diagnostic setting.
6. Navigate to `Storage accounts`.
7. Click on the storage account name noted in Step 5.
8. Under `Security + networking`, click `Encryption`.
9. Ensure `Customer-managed keys` is selected and a key is set.

Audit from Azure CLI

1. Get storage account id configured with log profile:

```
az monitor diagnostic-settings subscription list --subscription <subscription
id> --query 'value[*].storageAccountId'
```

2. Ensure the storage account is encrypted with CMK:

```
az storage account list --query "[?name=='<Storage Account Name>']"
```

In command output ensure `keySource` is set to `Microsoft.Keyvault` and `keyVaultProperties` is not set to `null`

Audit from PowerShell

```
Get-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage
account name>|select-object -ExpandProperty encryption|format-list
```

Ensure the value of `KeyVaultProperties` is not `null` or empty, and ensure `KeySource` is not set to `Microsoft.Storage`.

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:** fbb99e8e-e444-4da0-9ff1-75c92f5a85b2 **- Name:** 'Storage account containing the container with activity logs must be encrypted with BYOK'

Remediation:

Remediate from Azure Portal

1. Go to `Monitor`.
2. Select `Activity log`.
3. Select `Export Activity Logs`.
4. Select a `Subscription`.
5. Note the name of the `Storage Account` for the diagnostic setting.
6. Navigate to `Storage accounts`.
7. Click on the storage account.
8. Under `Security + networking`, click `Encryption`.
9. Next to `Encryption type`, select `Customer-managed keys`.
10. Complete the steps to configure a customer-managed key for encryption of the storage account.

Remediate from Azure CLI

```
az storage account update --name <name of the storage account> --resource-group <resource group for a storage account> --encryption-key-source=Microsoft.Keyvault --encryption-key-vault <Key Vault URI> --encryption-key-name <KeyName> --encryption-key-version <Key Version>
```

Remediate from PowerShell

```
Set-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage account name> -KeyvaultEncryption -KeyVaultUri <key vault URI> -KeyName <key name>
```

Default Value:

By default, for a storage account `keySource` is set to `Microsoft.Storage` allowing encryption with vendor Managed key and not a Customer Managed Key.

References:

1. 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
2. https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log?tabs=cli#managing-legacy-log-profiles

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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1041

7.1.1.4 Ensure that logging for Azure Key Vault is 'Enabled' (Automated)

Profile Applicability:

- Level 1

Description:

Enable AuditEvent logging for key vault instances to ensure interactions with key vaults are logged and available.

Rationale:

Monitoring how and when key vaults are accessed, and by whom, enables an audit trail of interactions with confidential information, keys, and certificates managed by Azure Key Vault. Enabling logging for Key Vault saves information in a user provided destination of either an Azure storage account or Log Analytics workspace. The same destination can be used for collecting logs for multiple Key Vaults.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, under `Monitoring`, go to `Diagnostic settings`.
3. Click `Edit setting` next to a diagnostic setting.
4. Ensure that a destination is configured.
5. Under `Category groups`, ensure that `audit` and `allLogs` are checked.

Audit from Azure CLI

List all key vaults

```
az keyvault list
```

For each keyvault `id`

```
az monitor diagnostic-settings list --resource <id>
```

Ensure that `storageAccountId` reflects your desired destination and that `categoryGroup` and `enabled` are set as follows in the sample outputs below.

```
"logs": [
{
    "categoryGroup": "audit",
    "enabled": true,
},
{
    "categoryGroup": "allLogs",
    "enabled": true,
}
```

Audit from PowerShell
List the key vault(s) in the subscription

```
Get-AzKeyVault
```

For each key vault, run the following:

```
Get-AzDiagnosticSetting -ResourceId <key_vault_id>
```

Ensure that `StorageAccountId`, `ServiceBusRuleId`, `MarketplacePartnerId`, or `WorkspaceId` is set as appropriate. Also, ensure that `enabled` is set to `true`, and that `categoryGroup` reflects both `audit` and `allLogs` category groups.

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:** cf820ca0-f99e-4f3e-84fb-66e913812d21 **- Name:** 'Resource logs in Key Vault should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. Select a Key vault.
3. Under `Monitoring`, select `Diagnostic settings`.
4. Click `Edit setting` to update an existing diagnostic setting, or `Add diagnostic setting` to create a new one.
5. If creating a new diagnostic setting, provide a name.
6. Configure an appropriate destination.
7. Under `Category groups`, check `audit` and `allLogs`.
8. Click `Save`.

Remediate from Azure CLI
To update an existing `Diagnostic Settings`

```
az monitor diagnostic-settings update --name "<diagnostic_setting_name>" --
resource <key_vault_id>
```

To create a new `Diagnostic Settings`

```
az monitor diagnostic-settings create --name "<diagnostic_setting_name>" --
resource <key_vault_id> --logs
"[{category:audit,enabled:true},{category:allLogs,enabled:true}]" --metrics
"[{category:AllMetrics,enabled:true}]" <[--event-hub <event_hub_ID> --event-
hub-rule <event_hub_auth_rule_ID> | --storage-account <storage_account_ID> |-
-workspace <log_analytics_workspace_ID> | --marketplace-partner-id
<solution_resource_ID>]>
```

Remediate from PowerShell
Create the `Log` settings object

```
$logSettings = @()
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
Category audit
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
Category allLogs
```

Create the `Metric` settings object

```
$metricSettings = @()
$metricSettings += New-AzDiagnosticSettingMetricSettingsObject -Enabled $true
-Category AllMetrics
```

Create the `Diagnostic Settings` for each `Key Vault`

```
New-AzDiagnosticSetting -Name "<diagnostic_setting_name>" -ResourceId
<key_vault_id> -Log $logSettings -Metric $metricSettings [-StorageAccountId
<storage_account_ID> | -EventHubName <event_hub_name> -
EventHubAuthorizationRuleId <event_hub_auth_rule_ID> | -WorkSpaceId <log
analytics workspace ID> | -MarketPlacePartnerId <full resource ID for third-
party solution>]
```

Default Value:

By default, Diagnostic AuditEvent logging is not enabled for Key Vault instances.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/general/howto-logging
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

Additional Information:

DEPRECATION WARNING

Retention rules for Key Vault logging is being migrated to Azure Storage Lifecycle Management. Retention rules should be set based on the needs of your organization and security or compliance frameworks. Please visit https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/migrate-to-azure-storage-lifecycle-policy?tabs=portal for detail on migrating your retention rules.

Microsoft has provided the following deprecation timeline:

March 31, 2023 – The Diagnostic Settings Storage Retention feature will no longer be available to configure new retention rules for log data. This includes using the portal, CLI PowerShell, and ARM and Bicep templates. If you have configured retention settings, you'll still be able to see and change them in the portal.

March 31, 2024 – You will no longer be able to use the API (CLI, Powershell, or templates), or Azure portal to configure retention setting unless you're changing them to 0. Existing retention rules will still be respected.

September 30, 2025 – All retention functionality for the Diagnostic Settings Storage Retention feature will be disabled across all environments.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

7.1.1.5 Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual)

Profile Applicability:

- Level 2

Description:

Ensure that network flow logs are captured and fed into a central log analytics workspace.

Retirement Notice

On September 30, 2027, network security group (NSG) flow logs will be retired. Starting June 30, 2025, it will no longer be possible to create new NSG flow logs. Azure recommends migrating to virtual network flow logs. Review https://azure.microsoft.com/en-gb/updates?id=Azure-NSG-flow-logs-Retirement for more information.

For virtual network flow logs, consider applying the recommendation `Ensure that virtual network flow logs are captured and sent to Log Analytics` in this section.

Rationale:

Network Flow Logs provide valuable insight into the flow of traffic around your network and feed into both Azure Monitor and Azure Sentinel (if in use), permitting the generation of visual flow diagrams to aid with analyzing for lateral movement, etc.

Impact:

The impact of configuring NSG Flow logs is primarily one of cost and configuration. If deployed, it will create storage accounts that hold minimal amounts of data on a 5-day lifecycle before feeding to Log Analytics Workspace. This will increase the amount of data stored and used by Azure Monitor.

Audit:

Audit from Azure Portal

1. Navigate to `Network Watcher`.
2. Under `Logs`, select `Flow logs`.
3. Click `Add filter`.
4. From the `Filter` drop-down, select `Flow log type`.
5. From the `Value` drop-down, check `Network security group` only.
6. Click `Apply`.
7. Ensure that at least one network security group flow log is listed and is configured to send logs to a `Log Analytics Workspace`.

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:** 27960feb-a23c-4577-8d36-ef8b5f35e0be **- Name:** 'All flow log resources should be in enabled state'
- **Policy ID:** c251913d-7d24-4958-af87-478ed3b9ba41 **- Name:** 'Flow logs should be configured for every network security group'
- **Policy ID:** 4c3c6c5f-0d47-4402-99b8-aa543dd8bcee **- Name:** 'Flow logs should be configured for every virtual network'

Remediation:

Remediate from Azure Portal

1. Navigate to `Network Watcher`.
2. Under `Logs`, select `Flow logs`.
3. Select `+ Create`.
4. Select the desired Subscription.
5. For `Flow log type`, select `Network security group`.
6. Select `+ Select target resource`.
7. Select `Network security group`.
8. Select a network security group.
9. Click `Confirm selection`.
10. Select or create a new Storage Account.
11. If using a v2 storage account, input the retention in days to retain the log.
12. Click `Next`.
13. Under `Analytics`, for `Flow log version`, select `Version 2`.
14. Check the box next to `Enable traffic analytics`.
15. Select a processing interval.
16. Select a `Log Analytics Workspace`.
17. Select `Next`.
18. Optionally add Tags.
19. Select `Review + create`.
20. Select `Create`.

Warning
The remediation policy creates remediation deployment and names them by concatenating the subscription name and the resource group name. The MAXIMUM permitted length of a deployment name is 64 characters. Exceeding this will cause the remediation task to fail.

Default Value:

By default Network Security Group logs are not sent to Log Analytics.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-4-enable-network-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	12.8 Deploy NetFlow Collection on Networking Boundary Devices Enable the collection of NetFlow and logging data on all network boundary devices.		●	●

7.1.1.6 Ensure that logging for Azure AppService 'HTTP logs' is enabled (Automated)

Profile Applicability:

- Level 2

Description:

Enable AppServiceHTTPLogs diagnostic log category for Azure App Service instances to ensure all http requests are captured and centrally logged.

Rationale:

Capturing web requests can be important supporting information for security analysts performing monitoring and incident response activities. Once logging, these logs can be ingested into SIEM or other central aggregation point for the organization.

Impact:

Log consumption and processing will incur additional cost.

Audit:

Audit from Azure Portal

1. Go to `App Services`.

For each `App Service`:

2. Under `Monitoring`, go to `Diagnostic settings`.
3. Ensure a diagnostic setting exists that logs `HTTP logs` to a destination aligned to your environment's approach to log consumption (event hub, storage account, etc. dependent on what is consuming the logs such as SIEM or other log aggregation utility).

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:** 91a78b24-f231-4a8a-8da9-02c35b2b6510 **- Name:** 'App Service apps should have resource logs enabled'
- **Policy ID:** d639b3af-a535-4bef-8dcf-15078cddf5e2 **- Name:** 'App Service app slots should have resource logs enabled'

Remediation:

Remediate from Azure Portal

1. Go to `App Services`.

For each `App Service`:

2. Under `Monitoring`, go to `Diagnostic settings`.
3. To update an existing diagnostic setting, click `Edit setting` against the setting. To create a new diagnostic setting, click `Add diagnostic setting` and provide a name for the new setting.
4. Check the checkbox next to `HTTP logs`.
5. Configure a destination based on your specific logging consumption capability (for example Stream to an event hub and then consuming with SIEM integration for Event Hub logging).
6. Click `Save`.

Default Value:

Not configured.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.7 Collect URL Request Audit Logs Collect URL request audit logs on enterprise assets, where appropriate and supported.		●	●
v7	7.6 Log all URL requests Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		●	●

7.1.1.7 Ensure that virtual network flow logs are captured and sent to Log Analytics (Manual)

Profile Applicability:

- Level 2

Description:

Ensure that virtual network flow logs are captured and fed into a central log analytics workspace.

Rationale:

Virtual network flow logs provide critical visibility into traffic patterns. Sending logs to a Log Analytics workspace enables centralized analysis, correlation, and alerting for faster threat detection and response.

Impact:

- Virtual network flow logs are charged per gigabyte of network flow logs collected and come with a free tier of 5 GB/month per subscription.
- If traffic analytics is enabled with virtual network flow logs, traffic analytics pricing applies at per gigabyte processing rates.
- The storage of logs is charged separately.

Audit:

Audit from Azure Portal

1. Go to `Network Watcher`.
2. Under `Logs`, select `Flow logs`.
3. Click `Add filter`.
4. From the `Filter` drop-down menu, select `Flow log type`.
5. From the `Value` drop-down menu, check `Virtual network` only.
6. Click `Apply`.
7. Ensure that at least one virtual network flow log is listed and is configured to send logs to a `Log Analytics Workspace`.

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:** 2f080164-9f4d-497e-9db6-416dc9f7b48a **- Name:** 'Network Watcher flow logs should have traffic analytics enabled'
- **Policy ID:** 4c3c6c5f-0d47-4402-99b8-aa543dd8bcee **- Name:** 'Audit flow logs configuration for every virtual network'

Remediation:

Remediate from Azure Portal

1. Go to `Network Watcher`.
2. Under `Logs`, click `Flow logs`.
3. Click `+ Create`.
4. Select a subscription.
5. Next to `Flow log type`, select `Virtual network`.
6. Click `+ Select target resource`.
7. Select `Virtual network`.
8. Select a virtual network.
9. Click `Confirm selection`.
10. Select a storage account, or create a new storage account.
11. Set the retention in days for the storage account.
12. Click `Next`.
13. Under `Analytics`, for `Flow logs version`, select `Version 2`.
14. Check the box next to `Enable traffic analytics`.
15. Select a processing interval.
16. Select a `Log Analytics Workspace`.
17. Click `Next`.
18. Optionally, add `Tags`.
19. Click `Review + create`.
20. Click `Create`.
21. Repeat steps 1-20 for each subscription or virtual network requiring remediation.

References:

1. https://learn.microsoft.com/en-us/azure/network-watcher/vnet-flow-logs-overview
2. https://learn.microsoft.com/en-us/azure/network-watcher/vnet-flow-logs-cli

Additional Information:

On September 30, 2027, NSG flow logs will be retired, and creating new NSG flow logs will no longer be possible after June 30, 2025. Azure recommends migrating to virtual network flow logs, which address NSG flow log limitations. After retirement, traffic analytics using NSG flow logs will no longer be supported, and existing NSG flow log resources will be deleted. Previously collected NSG flow log records will remain available per their retention policies. For details, see the official announcement: https://azure.microsoft.com/en-gb/updates?id=Azure-NSG-flow-logs-Retirement.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	12.8 Deploy NetFlow Collection on Networking Boundary Devices Enable the collection of NetFlow and logging data on all network boundary devices.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
		M1047

7.1.1.8 Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination (Manual)

Profile Applicability:

- Level 2

Description:

Ensure that a Microsoft Entra diagnostic setting is configured to send Microsoft Graph activity logs to a suitable destination, such as a Log Analytics workspace, storage account, or event hub. This enables centralized monitoring and analysis of all HTTP requests that the Microsoft Graph service receives and processes for a tenant.

Rationale:

Microsoft Graph activity logs provide visibility into HTTP requests made to the Microsoft Graph service, helping detect unauthorized access, suspicious activity, and security threats. Configuring diagnostic settings in Microsoft Entra ensures these logs are collected and sent to an appropriate destination for monitoring, analysis, and retention.

Impact:

A Microsoft Entra ID P1 or P2 tenant license is required to access the Microsoft Graph activity logs.

The amount of data logged and, thus, the cost incurred can vary significantly depending on the tenant size and the applications in your tenant that interact with the Microsoft Graph APIs.

See the following pricing calculations for respective services:

- Log Analytics: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cost-logs#pricing-model.
- Azure Storage: https://azure.microsoft.com/en-gb/pricing/details/storage/blobs/.
- Event Hubs: https://azure.microsoft.com/en-gb/pricing/details/event-hubs/

Audit:

Audit from Azure Portal

1. Go to `Microsoft Entra ID`.
2. Under `Monitoring`, click `Diagnostic settings`.
3. Next to each diagnostic setting, click `Edit setting`, and review the selected log categories and destination details.
4. Ensure that at least one diagnostic setting is configured to send `MicrosoftGraphActivityLogs` to an appropriate destination.

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Entra ID`.
2. Under `Monitoring`, click `Diagnostic settings`.
3. Click `+ Add diagnostic setting`.
4. Provide a `Diagnostic setting name`.
5. Under `Logs > Categories`, check the box next to `MicrosoftGraphActivityLogs`.
6. Configure an appropriate destination for the logs.
7. Click `Save`.

Default Value:

By default, Microsoft Entra diagnostic settings do not exist.

References:

1. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-configure-diagnostic-settings
2. https://learn.microsoft.com/en-us/graph/microsoft-graph-activity-logs-overview
3. https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cost-logs#pricing-model
4. https://azure.microsoft.com/en-gb/pricing/details/storage/blobs/
5. https://azure.microsoft.com/en-gb/pricing/details/event-hubs/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
		M1047

7.1.1.9 Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination (Manual)

Profile Applicability:

- Level 2

Description:

Ensure that a Microsoft Entra diagnostic setting is configured to send Microsoft Entra activity logs to a suitable destination, such as a Log Analytics workspace, storage account, or event hub. This enables centralized monitoring and analysis of Microsoft Entra activity logs.

Rationale:

Microsoft Entra activity logs enables you to assess many aspects of your Microsoft Entra tenant. Configuring diagnostic settings in Microsoft Entra ensures these logs are collected and sent to an appropriate destination for monitoring, analysis, and retention.

Impact:

To export sign-in data, your organization needs an Azure AD P1 or P2 license.

The amount of data logged and, thus, the cost incurred can vary significantly depending on the tenant size.

See the following pricing calculations for respective services:

- Log Analytics: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cost-logs#pricing-model.
- Azure Storage: https://azure.microsoft.com/en-gb/pricing/details/storage/blobs/.
- Event Hubs: https://azure.microsoft.com/en-gb/pricing/details/event-hubs/

Audit:

Audit from Azure Portal

1. Go to `Microsoft Entra ID`.
2. Under `Monitoring`, click `Diagnostic settings`.
3. Next to each diagnostic setting, click `Edit setting`, and review the selected log categories and destination details.
4. Ensure that at least one diagnostic setting is configured to send the following logs to an appropriate destination:
    - `AuditLogs`
    - `SignInLogs`
    - `NonInteractiveUserSignInLogs`

    - ServicePrincipalSignInLogs
    - ManagedIdentitySignInLogs
    - ProvisioningLogs
    - ADFSSignInLogs
    - RiskyUsers
    - UserRiskEvents
    - NetworkAccessTrafficLogs
    - RiskyServicePrincipals
    - ServicePrincipalRiskEvents
    - EnrichedOffice365AuditLogs
    - MicrosoftGraphActivityLogs
    - RemoteNetworkHealthLogs
    - NetworkAccessAlerts

Remediation:

Remediate from Azure Portal

1. Go to Microsoft Entra ID.
2. Under Monitoring, click Diagnostic settings.
3. Click + Add diagnostic setting.
4. Provide a Diagnostic setting name.
5. Under Logs > Categories, check the box next to each of the following logs:
    - AuditLogs
    - SignInLogs
    - NonInteractiveUserSignInLogs
    - ServicePrincipalSignInLogs
    - ManagedIdentitySignInLogs
    - ProvisioningLogs
    - ADFSSignInLogs
    - RiskyUsers
    - UserRiskEvents
    - NetworkAccessTrafficLogs
    - RiskyServicePrincipals
    - ServicePrincipalRiskEvents
    - EnrichedOffice365AuditLogs
    - MicrosoftGraphActivityLogs
    - RemoteNetworkHealthLogs
    - NetworkAccessAlerts
6. Configure an appropriate destination for the logs.
7. Click Save.

Default Value:

By default, Microsoft Entra diagnostic settings do not exist.

References:

1. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-configure-diagnostic-settings
2. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-access-activity-logs?tabs=microsoft-entra-activity-logs%2Carchive-activity-logs-to-a-storage-account

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
		M1047

7.1.1.10 Ensure that Intune logs are captured and sent to Log Analytics (Manual)

Profile Applicability:

- Level 2

Description:

Ensure that Intune logs are captured and fed into a central log analytics workspace.

Rationale:

Intune includes built-in logs that provide information about your environments. Sending logs to a Log Analytics workspace enables centralized analysis, correlation, and alerting for faster threat detection and response.

Impact:

A Microsoft Intune plan is required to access Intune: https://www.microsoft.com/en-gb/security/business/microsoft-intune-pricing.

The amount of data logged and, thus, the cost incurred can vary significantly depending on the tenant size.

For information on Log Analytics workspace costs, visit: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cost-logs.

Audit:

Audit from Azure Portal

1. Go to `Intune`.
2. Click `Reports`.
3. Under `Azure monitor`, click `Diagnostic settings`.
4. Next to each diagnostic setting, click `Edit setting`, and review the selected log categories and destination details.
5. Ensure that at least one diagnostic setting is configured to send the following logs to a Log Analytics workspace:
    - `AuditLogs`
    - `OperationalLogs`
    - `DeviceComplianceOrg`
    - `Devices`
    - `Windows365AuditLogs`

Remediation:

Remediate from Azure Portal

1. Go to `Intune`.
2. Click `Reports`.
3. Under `Azure monitor`, click `Diagnostic settings`.
4. Click `+ Add diagnostic setting`.
5. Provide a `Diagnostic setting name`.
6. Under `Logs > Categories`, check the box next to each of the following logs:
    - `AuditLogs`
    - `OperationalLogs`
    - `DeviceComplianceOrg`
    - `Devices`
    - `Windows365AuditLogs`
7. Under `Destination details`, check the box next to `Send to Log Analytics workspace`.
8. Select a `Subscription`.
9. Select a `Log Analytics workspace`.
10. Click `Save`.

Default Value:

By default, Intune diagnostic settings do not exist.

References:

1. https://learn.microsoft.com/en-us/mem/intune/fundamentals/review-logs-using-azure-monitor
2. https://www.microsoft.com/en-gb/security/business/microsoft-intune-pricing
3. https://learn.microsoft.com/en-us/azure/azure-monitor/logs/cost-logs

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
		M1047

7.1.2 Monitoring using Activity Log Alerts

The recommendations provided in this section are intended to provide entry-level alerting for crucial activities on a tenant account. These recommended activities **should** be tuned to your needs. By default, each of these Activity Log Alerts tends to guide the reader to alerting at the "Subscription-wide" level which will capture and alert on rules triggered by all resources and resource groups contained within a subscription. This is not an ideal rule set for Alerting within larger and more complex organizations.

While this section provides recommendations for the creation of **Activity Log Alerts** specifically, Microsoft Azure supports four different types of alerts:

- Metric Alerts
- Log Alerts
- Activity Log Alerts
- Smart Detection Alerts

All Azure services (Microsoft provided or otherwise) that can generate alerts are assigned a "Resource provider namespace" when they are registered in an Azure tenant. The recommendations in this section are in no way exhaustive of the plethora of available "Providers" or "Resource Types." The Resource Providers that are registered in your Azure Tenant can be located in your Subscription. Each registered Provider in your environment **may** have available "Conditions" to raise alerts via Activity Log Alerts. These providers should be considered for inclusion in Activity Log Alert rules of your own making.

To view the registered resource providers in your Subscription(s), use this guide:

- https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-providers-and-types

If you wish to create custom alerting rules for Activity Log Alerts or other alert types, please refer to Microsoft documentation:

- https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule

7.1.2.1 Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create Policy Assignment event.

Rationale:

Monitoring for create policy assignment events gives insight into changes done in "Azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Authorization/policyAssignments/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create policy assignment'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Authorization/policyAssignments/write` in the output. If it's missing, generate a finding.

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Authorization/policyAssignments/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

If the output is empty, an `alert rule` for `Create Policy Assignments` is not configured.

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:** c5447c04-a4d7-4ba8-a263-c9ee321a6858 **- Name:** 'An activity log alert should exist for specific Policy operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create policy assignment (Policy assignment)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Authorization/policyAssignments/write and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription ID> --action-group <action group ID>
```

Remediate from PowerShell
Create the `conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Authorization/policyAssignments/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Get the `Action Group` information and store it in a variable, then create a new `Action` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` variable.

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Authorization/policyAssignments/write`

```
New-AzActivityLogAlert -Name "<activity alert rule name>" -ResourceGroupName
"<resource group name>" -Condition $conditions -Scope $scope -Location global
-Action $actionObject -Subscription <subscription ID> -Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
6. https://docs.microsoft.com/en-in/rest/api/policy/policy-assignments
7. https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.2 Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Policy Assignment event.

Rationale:

Monitoring for delete policy assignment events gives insight into changes done in "azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Authorization/policyAssignments/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete policy assignment'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Authorization/policyAssignments/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Authorization/policyAssignments/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** c5447c04-a4d7-4ba8-a263-c9ee321a6858 **- Name:** 'An activity log alert should exist for specific Policy operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete policy assignment (Policy assignment)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Authorization/policyAssignments/delete and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the conditions object

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Authorization/policyAssignments/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Action` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` variable.

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Authorization/policyAssignments/delete`.

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
2. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
5. https://azure.microsoft.com/en-us/services/blueprints/

Additional Information:

This log alert also applies for Azure Blueprints.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.3 Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)

Profile Applicability:

- Level 1

Description:

Create an Activity Log Alert for the Create or Update Network Security Group event.

Rationale:

Monitoring for Create or Update Network Security Group events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/networkSecurityGroups/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create or Update Network Security Group'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/networkSecurityGroups/write` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/networkSecurityGroups/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create or Update Network Security Group (Network Security Group)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/write and level=verbose
--scope "/subscriptions/<subscription ID>" --name "<activity log rule name>"
--subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/networkSecurityGroups/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/networkSecurityGroups/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.4 Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Network Security Group event.

Rationale:

Monitoring for "Delete Network Security Group" events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/networkSecurityGroups/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete Network Security Group'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/networkSecurityGroups/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/networkSecurityGroups/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete Network Security Group (Network Security Group)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/delete and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/networkSecurityGroups/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/networkSecurityGroups/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.5 Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update Security Solution event.

Rationale:

Monitoring for Create or Update Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Security/securitySolutions/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create or Update Security Solutions'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Security/securitySolutions/write` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Security/securitySolutions/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create or Update Security Solutions (Security Solutions)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/write and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Security/securitySolutions/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Security/securitySolutions/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.6 Ensure that Activity Log Alert exists for Delete Security Solution (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Security Solution event.

Rationale:

Monitoring for Delete Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Security/securitySolutions/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete Security Solutions'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Security/securitySolutions/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Security/securitySolutions/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete Security Solutions (Security Solutions)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/delete and level=<verbose
| information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Security/securitySolutions/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Security/securitySolutions/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.7 Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update SQL Server Firewall Rule event.

Rationale:

Monitoring for Create or Update SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Sql/servers/firewallRules/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create/Update server firewall rule'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Sql/servers/firewallRules/write` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Sql/servers/firewallRules/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create/Update server firewall rule (Server Firewall Rule)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/write and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Sql/servers/firewallRules/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Sql/servers/firewallRules/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.8 Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the "Delete SQL Server Firewall Rule."

Rationale:

Monitoring for Delete SQL Server Firewall Rule events gives insight into SQL network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Sql/servers/firewallRules/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete server firewall rule'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Sql/servers/firewallRules/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Sql/servers/firewallRules/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete server firewall rule (Server Firewall Rule)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/delete and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Sql/servers/firewallRules/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Sql/servers/firewallRules/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.9 Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update Public IP Addresses rule.

Rationale:

Monitoring for Create or Update Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/publicIPAddresses/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create or Update Public Ip Address'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/publicIPAddresses/write` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/publicIPAddresses/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** 1513498c-3091-461a-b321-e9b433218d28 **- Name:** 'Enable logging by category group for Public IP addresses (microsoft.network/publicipaddresses) to Log Analytics'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create or Update Public Ip Address (Public Ip Address)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/publicIPAddresses/write and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/publicIPAddresses/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/publicIPAddresses/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.10 Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Public IP Address rule.

Rationale:

Monitoring for Delete Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/publicIPAddresses/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete Public Ip Address'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/publicIPAddresses/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/publicIPAddresses/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

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:** 1513498c-3091-461a-b321-e9b433218d28 **- Name:** 'Enable logging by category group for Public IP addresses (microsoft.network/publicipaddresses) to Log Analytics'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete Public Ip Address (Public Ip Address)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/publicIPAddresses/delete and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/publicIPAddresses/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/publicIPAddresses/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

7.1.2.11 Ensure that an Activity Log Alert exists for Service Health (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for Service Health.

Rationale:

Monitoring for Service Health events provides insight into service issues, planned maintenance, security advisories, and other changes that may affect the Azure services and regions in use.

Impact:

There is no charge for creating activity log alert rules.

Audit:

Audit from Azure Portal

1. Go to `Monitor`.
2. Click `Alerts`.
3. Click `Alert rules`.
4. Ensure an alert rule exists for a subscription with `Condition` set to `Service names=All, Event types=All` and `Target resource type` set to `Subscription`.
5. If an alert rule is found for step 4, click the name of the alert rule.
6. Ensure the `Actions` panel displays an action group configured to notify appropriate personnel.
7. Repeat steps 1-6 for each subscription.

Audit from Azure CLI

Run the following command to list activity log alerts:

```
az monitor activity-log alert list --subscription <subscription-id>
```

For each activity log alert, run the following command:

```
az monitor activity-log alert show --subscription <subscription-id> --
resource-group <resource-group> --activity-log-alert-name <activity-log-
alert>
```

Ensure an alert exists for `ServiceHealth` with `scopes` set to a subscription ID.
Repeat for each subscription.

Audit from PowerShell
Run the following command to locate `ServiceHealth` alert rules for a subscription:

```
Get-AzActivityLogAlert -SubscriptionId <subscription-id> | where-object
{$_.ConditionAllOf.Equal -match "ServiceHealth"} | select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Ensure that at least one `ServiceHealth` alert rule is returned.
Repeat for each subscription.

Remediation:

Remediate from Azure Portal

1. Go to `Monitor`.
2. Click `Alerts`.
3. Click `+ Create`.
4. Select `Alert rule` from the drop-down menu.
5. Choose a subscription.
6. Click `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Service health`.
10. Click `Apply`.
11. Open the drop-down menu next to `Event types`.
12. Check the box next to `Select all`.
13. Select the `Actions` tab.
14. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
15. Follow the prompts to choose or create an action group.
16. Select the `Details` tab.
17. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
18. Click `Review + create`.
19. Click `Create`.
20. Repeat steps 1-19 for each subscription requiring remediation.

Remediate from Azure CLI
For each subscription requiring remediation, run the following command to create a `ServiceHealth` alert rule for a subscription:

```
az monitor activity-log alert create --subscription <subscription-id> --
resource-group <resource-group> --name <alert-rule> --condition
category=ServiceHealth and properties.incidentType=Incident --scope
/subscriptions/<subscription-id> --action-group <action-group>
```

Remediate from PowerShell
Create the `Conditions` object:

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Field category -Equal ServiceHealth
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Field properties.incidentType -Equal Incident
```

Retrieve the `Action Group` information and store in a variable:

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource-group> -Name
<action-group>
```

Create the `Actions` object:

```
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object:

```
$scope = "/subscriptions/<subscription-id>"
```

Create the activity log alert rule:

```
New-AzActivityLogAlert -Name <alert-rule> -ResourceGroupName <resource-group>
-Condition $conditions -Scope $scope -Location global -Action $actionObject -
Subscription <subscription-id> -Enabled $true
```

Repeat for each subscription requiring remediation.

Default Value:

By default, no monitoring alerts are created.

References:

1. https://learn.microsoft.com/en-us/azure/service-health/overview
2. https://learn.microsoft.com/en-us/azure/service-health/alerts-activity-log-service-notifications-portal
3. https://azure.microsoft.com/en-gb/pricing/details/monitor/#faq
4. https://learn.microsoft.com/en-us/cli/azure/monitor/activity-log/alert
5. https://learn.microsoft.com/en-us/powershell/module/az.monitor/get-azactivitylogalert
6. https://learn.microsoft.com/en-us/powershell/module/az.monitor/new-azactivitylogalert

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
		M1047

7.1.3 Configuring Application Insights

7.1.3.1 Ensure Application Insights are Configured (Automated)

Profile Applicability:

- Level 2

Description:

Application Insights within Azure act as an Application Performance Monitoring solution providing valuable data into how well an application performs and additional information when performing incident response. The types of log data collected include application metrics, telemetry data, and application trace logging data providing organizations with detailed information about application activity and application transactions. Both data sets help organizations adopt a proactive and retroactive means to handle security and performance related metrics within their modern applications.

Rationale:

Configuring Application Insights provides additional data not found elsewhere within Azure as part of a much larger logging and monitoring program within an organization's Information Security practice. The types and contents of these logs will act as both a potential cost saving measure (application performance) and a means to potentially confirm the source of a potential incident (trace logging). Metrics and Telemetry data provide organizations with a proactive approach to cost savings by monitoring an application's performance, while the trace logging data provides necessary details in a reactive incident response scenario by helping organizations identify the potential source of an incident within their application.

Impact:

Because Application Insights relies on a Log Analytics Workspace, an organization will incur additional expenses when using this service.

Audit:
Audit from Azure Portal

1. Navigate to `Application Insights`.
2. Ensure an `Application Insights` service is configured and exists.

Audit from Azure CLI

```
az monitor app-insights component show --query "[].{ID:appId, Name:name,
Tenant:tenantId, Location:location, Provisioning_State:provisioningState}"
```

Ensure the above command produces output, otherwise `Application Insights` has not been configured.
Audit from PowerShell

```
Get-AzApplicationInsights|select
location,name,appid,provisioningState,tenanted
```

Remediation:

Remediate from Azure Portal

1. Navigate to `Application Insights`.
2. Under the `Basics` tab within the `PROJECT DETAILS` section, select the `Subscription`.
3. Select the `Resource group`.
4. Within the `INSTANCE DETAILS`, enter a `Name`.
5. Select a `Region`.
6. Next to `Resource Mode`, select `Workspace-based`.
7. Within the `WORKSPACE DETAILS`, select the `Subscription` for the log analytics workspace.
8. Select the appropriate `Log Analytics Workspace`.
9. Click `Next:Tags >`.
10. Enter the appropriate `Tags` as `Name`, `Value` pairs.
11. Click `Next:Review+Create`.
12. Click `Create`.

Remediate from Azure CLI

```
az monitor app-insights component create --app <app name> --resource-group
<resource group name> --location <location> --kind "web" --retention-time
<INT days to retain logs> --workspace <log analytics workspace ID> --
subscription <subscription ID>
```

Remediate from PowerShell

```
New-AzApplicationInsights -Kind "web" -ResourceGroupName <resource group
name> -Name <app insights name> -location <location> -RetentionInDays <INT
days to retain logs> -SubscriptionID <subscription ID> -WorkspaceResourceId
<log analytics workspace ID>
```

Default Value:

Application Insights are not enabled by default.

References:

1. https://learn.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1606	TA0006	M1047

7.1.4 Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)

Profile Applicability:

- Level 1

Description:

Resource Logs capture activity to the data access plane while the Activity log is a subscription-level log for the control plane. Resource-level diagnostic logs provide insight into operations that were performed within that resource itself; for example, reading or updating a secret from a Key Vault. Currently, 95 Azure resources support Azure Monitoring (See the more information section for a complete list), including Network Security Groups, Load Balancers, Key Vault, AD, Logic Apps, and CosmosDB. The content of these logs varies by resource type.

A number of back-end services were not configured to log and store Resource Logs for certain activities or for a sufficient length. It is crucial that monitoring is correctly configured to log all relevant activities and retain those logs for a sufficient length of time. Given that the mean time to detection in an enterprise is 240 days, a minimum retention period of two years is recommended.

Rationale:

A lack of monitoring reduces the visibility into the data plane, and therefore an organization's ability to detect reconnaissance, authorization attempts or other malicious activity. Unlike Activity Logs, Resource Logs are not enabled by default. Specifically, without monitoring it would be impossible to tell which entities had accessed a data store that was breached. In addition, alerts for failed attempts to access APIs for Web Services or Databases are only possible when logging is enabled.

Impact:

Costs for monitoring varies with Log Volume. Not every resource needs to have logging enabled. It is important to determine the security classification of the data being processed by the given resource and adjust the logging based on which events need to be tracked. This is typically determined by governance and compliance requirements.

Audit:

Audit from Azure Portal
The specific steps for configuring resources within the Azure console vary depending on resource, but typically the steps are:

1. Go to the resource
2. Click on Diagnostic settings
3. In the blade that appears, click "Add diagnostic setting"

4. Configure the diagnostic settings
5. Click on Save

Audit from Azure CLI

List all `resources` for a `subscription`

```
az resource list --subscription <subscription id>
```

For each `resource` run the following

```
az monitor diagnostic-settings list --resource <resource ID>
```

An empty result means a `diagnostic settings` is not configured for that resource. An error message means a `diagnostic settings` is not supported for that resource.

Audit from PowerShell

Get a list of `resources` in a `subscription` context and store in a variable

```
$resources = Get-AzResource
```

Loop through each `resource` to determine if a diagnostic setting is configured or not.

```
foreach ($resource in $resources) {$diagnosticSetting = Get-
AzDiagnosticSetting -ResourceId $resource.id -ErrorAction "SilentlyContinue";
if ([string]::IsNullOrEmpty($diagnosticSetting)) {$message = "Diagnostic
Settings not configured for resource: " + $resource.Name;Write-Output
$message}else{$diagnosticSetting}}
```

A result of `Diagnostic Settings not configured for resource: <resource name>` means a `diagnostic settings` is not configured for that resource. Otherwise, the output of the above command will show configured `Diagnostic Settings` for a resource.

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:** cf820ca0-f99e-4f3e-84fb-66e913812d21 **- Name:** 'Resource logs in Key Vault should be enabled'
- **Policy ID:** 91a78b24-f231-4a8a-8da9-02c35b2b6510 **- Name:** 'App Service apps should have resource logs enabled'
- **Policy ID:** 428256e6-1fac-4f48-a757-df34c2b3336d **- Name:** 'Resource logs in Batch accounts should be enabled'
- **Policy ID:** 057ef27e-665e-4328-8ea3-04b3122bd9fb **- Name:** 'Resource logs in Azure Data Lake Store should be enabled'
- **Policy ID:** c95c74d9-38fe-4f0d-af86-0c7d626a315c **- Name:** 'Resource logs in Data Lake Analytics should be enabled'
- **Policy ID:** 83a214f7-d01a-484b-91a9-ed54470c9a6a **- Name:** 'Resource logs in Event Hub should be enabled'
- **Policy ID:** 383856f8-de7f-44a2-81fc-e5135b5c2aa4 **- Name:** 'Resource logs in IoT Hub should be enabled'

- **Policy ID:** 34f95f76-5386-4de7-b824-0d8478470c9d **- Name:** 'Resource logs in Logic Apps should be enabled'
- **Policy ID:** b4330a05-a843-4bc8-bf9a-cacce50c67f4 **- Name:** 'Resource logs in Search services should be enabled'
- **Policy ID:** f8d36e2f-389b-4ee4-898d-21aeb69a0f45 **- Name:** 'Resource logs in Service Bus should be enabled'
- **Policy ID:** f9be5368-9bf5-4b84-9e0a-7850da98bb46 **- Name:** 'Resource logs in Azure Stream Analytics should be enabled'

Remediation:

Azure Subscriptions should log every access and operation for all resources.
Logs should be sent to Storage and a Log Analytics Workspace or equivalent third-party system. Logs should be kept in readily-accessible storage for a minimum of one year, and then moved to inexpensive cold storage for a duration of time as necessary. If retention policies are set but storing logs in a Storage Account is disabled (for example, if only Event Hubs or Log Analytics options are selected), the retention policies have no effect. Enable all monitoring at first, and then be more aggressive moving data to cold storage if the volume of data becomes a cost concern.
Remediate from Azure Portal
The specific steps for configuring resources within the Azure console vary depending on resource, but typically the steps are:

1. Go to the resource
2. Click on Diagnostic settings
3. In the blade that appears, click "Add diagnostic setting"
4. Configure the diagnostic settings
5. Click on Save

Remediate from Azure CLI
For each `resource`, run the following making sure to use a `resource` appropriate JSON encoded `category` for the `--logs` option.

```
az monitor diagnostic-settings create --name <diagnostic settings name> --
resource <resource ID> --logs "[{category:<resource specific
category>,enabled:true,rentention-policy:{enabled:true,days:180}}]" --metrics
"[{category:AllMetrics,enabled:true,retention-
policy:{enabled:true,days:180}}]" <[--event-hub <event hub ID> --event-hub-
rule <event hub auth rule ID> | --storage-account <storage account ID> |--
workspace <log analytics workspace ID> | --marketplace-partner-id <full
resource ID of third-party solution>]>
```

Remediate from PowerShell
Create the `log` settings object

```
$logSettings = @()
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category <resource
specific category>
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category <resource
specific category number 2>
```

Create the `metric` settings object

```
$metricSettings = @()
$metricSettings += New-AzDiagnosticSettingMetricSettingsObject -Enabled $true
-RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category AllMetrics
```

Create the diagnostic setting for a specific resource

```
New-AzDiagnosticSetting -Name "<diagnostic settings name>" -ResourceId
<resource ID> -Log $logSettings -Metric $metricSettings
```

Default Value:

By default, Azure Monitor Resource Logs are 'Disabled' for all resources.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis
3. https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/monitor-azure-resource
4. Supported Log Categories: https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs-categories
5. Logs and Audit - Fundamentals: https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit
6. Collecting Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-activity-logs
7. Key Vault Logging: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-logging
8. Monitor Diagnostic Settings: https://docs.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest
9. Overview of Diagnostic Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-overview
10. Supported Services for Diagnostic Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-schema
11. Diagnostic Logs for CDNs: https://docs.microsoft.com/en-us/azure/cdn/cdn-azure-diagnostic-logs

Additional Information:

For an up-to-date list of Azure resources which support Azure Monitor, refer to the "Supported Log Categories" reference.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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.		●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

7.1.5 Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Manual)

Profile Applicability:

- Level 2

Description:

The use of Basic or Free SKUs in Azure whilst cost effective have significant limitations in terms of what can be monitored and what support can be realized from Microsoft. Typically, these SKU's do not have a service SLA and Microsoft may refuse to provide support for them. Consequently Basic/Free SKUs should never be used for production workloads.

Rationale:

Typically, production workloads need to be monitored and should have an SLA with Microsoft, using Basic SKUs for any deployed product will mean that that these capabilities do not exist.

The following resource types should use standard SKUs as a minimum.

- Public IP Addresses
- Network Load Balancers
- REDIS Cache
- SQL PaaS Databases
- VPN Gateways

Impact:

The impact of enforcing Standard SKU's is twofold

1. There will be a cost increase
2. The monitoring and service level agreements will be available and will support the production service.

All resources should be either tagged or in separate Management Groups/Subscriptions

Audit:

This needs to be audited by Azure Policy (one for each resource type) and denied for each artifact that is production.
Audit from Azure Portal

1. Open `Azure Resource Graph Explorer`
2. Click `New query`

3. Paste the following into the query window:

```
Resources
| where sku contains 'Basic' or sku contains 'consumption'
| order by type
```

4. Click `Run query` then evaluate the results in the results window.
5. Ensure that no production artifacts are returned.

Audit from Azure CLI

```
az graph query -q "Resources | where sku contains 'Basic' or sku contains
'consumption' | order by type"
```

Alternatively, to filter on a specific resource group:

```
az graph query -q "Resources | where resourceGroup == '<resourceGroupName>' |
where sku contains 'Basic' or sku contains 'consumption' | order by type"
```

Ensure that no production artifacts are returned.

Audit from PowerShell

```
Get-AzResource | ?{ $_.Sku -EQ "Basic"}
```

Ensure that no production artifacts are returned.

Remediation:

Each resource has its own process for upgrading from basic to standard SKUs that should be followed if required.

- Public IP Address: https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-upgrade.
- Basic Load Balancer: https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-basic-upgrade-guidance.
- Azure Cache for Redis: https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-how-to-scale.
- Azure SQL Database: https://learn.microsoft.com/en-us/azure/azure-sql/database/scale-resources.
- VPN Gateway: https://learn.microsoft.com/en-us/azure/vpn-gateway/gateway-sku-resize.

Default Value:

Policy should enforce standard SKUs for the following artifacts:

- Public IP Addresses
- Network Load Balancers
- REDIS Cache
- SQL PaaS Databases

- VPN Gateways

References:

1. https://azure.microsoft.com/en-us/support/plans
2. https://azure.microsoft.com/en-us/support/plans/response/
3. https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-upgrade
4. https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-basic-upgrade-guidance
5. https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-how-to-scale
6. https://learn.microsoft.com/en-us/azure/azure-sql/database/scale-resources
7. https://learn.microsoft.com/en-us/azure/vpn-gateway/gateway-sku-resize

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported 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 Ensure Software is Supported by Vendor 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.	●	●	●

7.2 Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual)

Profile Applicability:

- Level 2

Description:

Resource Manager Locks provide a way for administrators to lock down Azure resources to prevent deletion of, or modifications to, a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and, when applied, will place restrictions on the resource for all users. These locks are very useful when there is an important resource in a subscription that users should not be able to delete or change. Locks can help prevent accidental and malicious changes or deletion.

Rationale:

As an administrator, it may be necessary to lock a subscription, resource group, or resource to prevent other users in the organization from accidentally deleting or modifying critical resources. The lock level can be set to to `CanNotDelete` or `ReadOnly` to achieve this purpose.

- `CanNotDelete` means authorized users can still read and modify a resource, but they cannot delete the resource.
- `ReadOnly` means authorized users can read a resource, but they cannot delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Impact:

There can be unintended outcomes of locking a resource. Applying a lock to a parent service will cause it to be inherited by all resources within. Conversely, applying a lock to a resource may not apply to connected storage, leaving it unlocked. Please see the documentation for further information.

Audit:

Audit from Azure Portal

1. Navigate to the specific Azure Resource or Resource Group.
2. Click on `Locks`.
3. Ensure the lock is defined with name and description, with type `Read-only` or `Delete` as appropriate.

Audit from Azure CLI
Review the list of all locks set currently:

```
az lock list --resource-group <resourcegroupname> --resource-name
<resourcename> --namespace <Namespace> --resource-type <type> --parent ""
```

Audit from PowerShell
Run the following command to list all resources.

```
Get-AzResource
```

For each resource, run the following command to check for Resource Locks.

```
Get-AzResourceLock -ResourceName <Resource Name> -ResourceType <Resource
Type> -ResourceGroupName <Resource Group Name>
```

Review the output of the `Properties` setting. Compliant settings will have the `CanNotDelete` or `ReadOnly` value.

Remediation:

Remediate from Azure Portal

1. Navigate to the specific Azure Resource or Resource Group.
2. For each mission critical resource, click on `Locks`.
3. Click `Add`.
4. Give the lock a name and a description, then select the type, `Read-only` or `Delete` as appropriate.
5. Click OK.

Remediate from Azure CLI
To lock a resource, provide the name of the resource, its resource type, and its resource group name.

```
az lock create --name <LockName> --lock-type <CanNotDelete/Read-only> --
resource-group <resourceGroupName> --resource-name <resourceName> --resource-
type <resourceType>
```

Remediate from PowerShell

```
Get-AzResourceLock -ResourceName <Resource Name> -ResourceType <Resource
Type> -ResourceGroupName <Resource Group Name> -Locktype <CanNotDelete/Read-
only>
```

Default Value:

By default, no locks are set.

References:

1. https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources
2. https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-subscription-governance#azure-resource-locks

3. https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-asset-management#am-4-limit-access-to-asset-management

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.	●	●	●

8 Networking Services

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

This section covers security recommendations to follow in order to set networking policies on an Azure subscription.

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#networking

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

8.1 Ensure that RDP access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where RDP is not explicitly required and narrowly configured for resources attached to a network security group, Internet-level access to Azure resources should be restricted or eliminated.

Rationale:

The potential security problem with using RDP over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on an Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Audit from Azure Portal

1. Go to `Network security groups`.
2. Under `Settings`, click `Inbound security rules`.
3. Ensure that no inbound security rule exists that matches the following:
    - Port: `3389` or range including 3389
    - Protocol: `TCP` or `Any`
    - Source: `0.0.0.0/0`, `Internet`, or `Any`
    - Action: `Allow`
4. Repeat steps 1-3 for each network security group.

To audit from Azure Resource Graph:

1. Go to `Resource Graph Explorer`.
2. Click `New query`.
3. Paste the following into the query window: *[next page]*

```
resources | where type =~ "microsoft.network/networksecuritygroups" |
project id, name, securityRule = properties.securityRules | mv-expand
securityRule | extend access = securityRule.properties.access,
direction = securityRule.properties.direction, protocol =
securityRule.properties.protocol, destinationPort =
case(isempty(securityRule.properties.destinationPortRange),
securityRule.properties.destinationPortRanges,
securityRule.properties.destinationPortRange), sourceAddress =
case(isempty(securityRule.properties.sourceAddressPrefix),
securityRule.properties.sourceAddressPrefixes,
securityRule.properties.sourceAddressPrefix) | where access =~ "Allow"
and direction =~ "Inbound" and protocol in~ ("tcp", "") | mv-expand
destinationPort | mv-expand sourceAddress | extend destinationPortMin =
toint(split(destinationPort, "-")[0]), destinationPortMax =
toint(split(destinationPort, "-")[-1]) | where (destinationPortMin <=
3389 and destinationPortMax >= 3389) or destinationPort == "" | where
sourceAddress in~ ("*", "0.0.0.0", "internet", "any") or sourceAddress
endswith "/0"
```

4. Click `Run query`.
5. Ensure that no results are returned.

Audit from Azure CLI

List network security groups with non-default security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that no network security group has an inbound security rule that matches the following:

```
"access" : "Allow"
"destinationPortRange" : "3389", "*", or "<range-including-3389>"
"direction" : "Inbound"
"protocol" : "TCP" or "*"
"sourceAddressPrefix" : "0.0.0.0/0", "Internet", or "*"
```

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:** 22730e10-96f6-4aac-ad84-9383d35b5917 **- Name:** 'Management ports should be closed on your virtual machines'

Remediation:

Remediate from Azure Portal

1. Go to `Network security groups`.
2. Under `Settings`, click `Inbound security rules`.
3. Check the box next to any inbound security rule matching:
    - Port: `3389` or range including 3389

- Protocol: `TCP` or `Any`
- Source: `0.0.0.0/0`, `Internet`, or `Any`
- Action: `Allow`

4. Click `Delete`.
5. Click `Yes`.

Remediate from Azure CLI
For each network security group rule requiring remediation, run the following command to delete a rule:

```
az network nsg rule delete --resource-group <resource-group> --nsg-name
<network-security-group> --name <rule>
```

Default Value:

By default, RDP access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries
3. Express Route: https://docs.microsoft.com/en-us/azure/expressroute/
4. Site-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
5. Point-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021.001	TA0001	M1035

8.2 Ensure that SSH access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

Rationale:

The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Audit from Azure Portal

1. Open the `Networking` blade for the specific Virtual machine in Azure portal
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for SSH such as
    - port = `22`,
    - protocol = `TCP` OR `ANY`,
    - Source = `Any` OR `Internet`

Audit from Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "22" or "*" or "[port range containing 22]"
"direction" : "Inbound"
"protocol" : "TCP" or "*"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

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:** 22730e10-96f6-4aac-ad84-9383d35b5917 **- Name:** 'Management ports should be closed on your virtual machines'

Remediation:

Where SSH is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.
For internal access to relevant resources, configure an encrypted network tunnel such as:
ExpressRoute
Site-to-site VPN
Point-to-site VPN

Default Value:

By default, SSH access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries
3. Express Route: https://docs.microsoft.com/en-us/azure/expressroute/
4. Site-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
5. Point-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1021.004	TA0001	M1035

8.3 Ensure that UDP access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

Rationale:

The potential security problem with broadly exposing UDP services over the Internet is that attackers can use DDoS amplification techniques to reflect spoofed UDP traffic from Azure Virtual Machines. The most common types of these attacks use exposed DNS, NTP, SSDP, SNMP, CLDAP and other UDP-based services as amplification sources for disrupting services of other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Audit from Azure Portal

1. Open the `Networking` blade for the specific Virtual machine in Azure portal
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for UDP such as

- protocol = `UDP`,
- Source = `Any` OR `Internet`

Audit from Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "*" or "[port range containing 53, 123, 161, 389,
1900, or other vulnerable UDP-based services]"
"direction" : "Inbound"
"protocol" : "UDP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Where UDP is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.
For internal access to relevant resources, configure an encrypted network tunnel such as:
ExpressRoute
Site-to-site VPN
Point-to-site VPN

Default Value:

By default, UDP access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices#secure-your-critical-azure-service-resources-to-only-your-virtual-networks
2. https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries
4. ExpressRoute: https://docs.microsoft.com/en-us/azure/expressroute/
5. Site-to-site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
6. Point-to-site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1095	TA0011	M1037

8.4 Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required and narrowly configured.

Rationale:

The potential security problem with using HTTP(S) over the Internet is that attackers can use various brute force techniques to gain access to Azure resources. Once the attackers gain access, they can use the resource as a launch point for compromising other resources within the Azure tenant.

Audit:

Audit from Azure Portal

1. For each VM, open the Networking blade
2. Verify that the INBOUND PORT RULES does not have a rule for HTTP(S) such as
    - port = `80`/ `443`,
    - protocol = `TCP`,
    - Source = `Any` OR `Internet`

Audit from Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "80/443" or "*" or "[port range containing 80/443]"
"direction" : "Inbound"
"protocol" : "TCP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Remediate from Azure Portal

1. Go to `Virtual machines`.
2. For each VM, open the `Networking` blade.
3. Click on `Inbound port rules`.
4. Delete the rule with:
    - Port = 80/443 OR [port range containing 80/443]
    - Protocol = TCP OR Any
    - Source = Any (*) OR IP Addresses(0.0.0.0/0) OR Service Tag(Internet)
    - Action = Allow

Remediate from Azure CLI

1. Run below command to list network security groups:

```
az network nsg list --subscription <subscription-id> --output table
```

2. For each network security group, run below command to list the rules associated with the specified port:

```
az network nsg rule list --resource-group <resource-group> --nsg-name
<nsg-name> --query "[?destinationPortRange=='80 or 443']"
```

3. Run the below command to delete the rule with:
    - Port = 80/443 OR [port range containing 80/443]
    - Protocol = TCP OR "*"
    - Source = Any (*) OR IP Addresses(0.0.0.0/0) OR Service Tag(Internet)
    - Action = Allow

```
az network nsg rule delete --resource-group <resource-group> --nsg-name
<nsg-name> --name <rule-name>
```

References:

1. Express Route: https://docs.microsoft.com/en-us/azure/expressroute/
2. Site-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
3. Point-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1190	TA0001	M1050

8.5 Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)

Profile Applicability:

- Level 2

Description:

Network Security Group Flow Logs should be enabled and the retention period set to greater than or equal to 90 days.

Retirement Notice

On September 30, 2027, network security group (NSG) flow logs will be retired. Starting June 30, 2025, it will no longer be possible to create new NSG flow logs. Azure recommends migrating to virtual network flow logs. Review https://azure.microsoft.com/en-gb/updates?id=Azure-NSG-flow-logs-Retirement for more information.

For virtual network flow logs, consider applying the recommendation `Ensure that virtual network flow log retention days is set to greater than or equal to 90` in this section.

Rationale:

Flow logs enable capturing information about IP traffic flowing in and out of network security groups. Logs can be used to check for anomalies and give insight into suspected breaches.

Impact:

This will keep IP traffic logs for longer than 90 days. As a level 2, first determine your need to retain data, then apply your selection here. As this is data stored for longer, your monthly storage costs will increase depending on your data use.

Audit:

Audit from Azure Portal

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the Logs section
3. Select each Network Security Group from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting `greater than 90 days`

Audit from Azure CLI

```
az network watcher flow-log show --resource-group <resourceGroup> --nsg
<NameorID of the NetworkSecurityGroup> --query 'retentionPolicy'
```

Ensure that `enabled` is set to `true` and `days` is set to `greater then or equal to 90`.

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:** 5e1cd26a-5090-4fdb-9d6a-84a90335e22d **- Name:** 'Configure network security groups to use specific workspace, storage account and flowlog retention policy for traffic analytics'

Remediation:

Remediate from Azure Portal

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the Logs section
3. Select each Network Security Group from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting `greater than 90 days`
6. Select your storage account in the `Storage account` field
7. Select `Save`

Remediate from Azure CLI

Enable the `NSG flow logs` and set the Retention (days) to greater than or equal to 90 days.

```
az network watcher flow-log configure --nsg <NameorID of the Network Security
Group> --enabled true --resource-group <resourceGroupName> --retention 91 --
storage-account <NameorID of the storage account to save flow logs>
```

Default Value:

By default, Network Security Group Flow Logs are `disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview
2. https://docs.microsoft.com/en-us/cli/azure/network/watcher/flow-log?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-6-configure-log-storage-retention

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v8	8.10 Retain Audit Logs Retain audit logs across enterprise assets for a minimum of 90 days.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

8.6 Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use (Automated)

Profile Applicability:

- Level 2

Description:

Enable Network Watcher for physical regions in Azure subscriptions.

Rationale:

Network diagnostic and visualization tools available with Network Watcher help users understand, diagnose, and gain insights to the network in Azure.

Impact:

There are additional costs per transaction to run and store network data. For high-volume networks these charges will add up quickly.

Audit:

Audit from Azure Portal

1. Use the Search bar to search for and click on the `Network Watcher` service.
2. From the Overview menu item, review each Network Watcher listed, and ensure that a network watcher is listed for each region in use by the subscription.

Audit from Azure CLI

```
az network watcher list --query
"[].{Location:location,State:provisioningState}" -o table
```

This will list all network watchers and their provisioning state.
Ensure `provisioningState` is `Succeeded` for each network watcher.

```
az account list-locations --query
"[?metadata.regionType=='Physical'].{Name:name,DisplayName:regionalDisplayNam
e}" -o table
```

This will list all physical regions that exist in the subscription.
Compare this list to the previous one to ensure that for each region in use, a network watcher exists with `provisioningState` set to `Succeeded`.

Audit from PowerShell
Get a list of Network Watchers

```
Get-AzNetworkWatcher
```

Make sure each watcher is set with the `ProvisioningState` setting set to `Succeeded` and all `Locations` that are in use by the subscription are using a watcher.

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:** b6e2945c-0b7b-40f5-9233-7a5323b5cdc6 **- Name:** 'Network Watcher should be enabled'

Remediation:

Opting out of Network Watcher automatic enablement is a permanent change. Once you opt-out you cannot opt-in without contacting support.
To manually enable Network Watcher in each region where you want to use Network Watcher capabilities, follow the steps below.
Remediate from Azure Portal

1. Use the Search bar to search for and click on the `Network Watcher` service.
2. Click `Create`.
3. Select a `Region` from the drop-down menu.
4. Click `Add`.

Remediate from Azure CLI

```
az network watcher configure --locations <region> --enabled true --resource-group <resource_group>
```

Default Value:

Network Watcher is automatically enabled. When you create or update a virtual network in your subscription, Network Watcher will be enabled automatically in your Virtual Network's region. There is no impact to your resources or associated charge for automatically enabling Network Watcher.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
2. https://learn.microsoft.com/en-us/cli/azure/network/watcher?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/cli/azure/network/watcher?view=azure-cli-latest#az-network-watcher-configure
4. https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-create
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-4-enable-network-logging-for-security-investigation
6. https://azure.microsoft.com/en-ca/pricing/details/network-watcher/

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.		●	●
v8	12.4 Establish and Maintain Architecture Diagram(s) Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

8.7 Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual)

Profile Applicability:

- Level 1

Description:

Public IP Addresses provide tenant accounts with Internet connectivity for resources contained within the tenant. During the creation of certain resources in Azure, a Public IP Address may be created. All Public IP Addresses within the tenant should be periodically reviewed for accuracy and necessity.

Rationale:

Public IP Addresses allocated to the tenant should be periodically reviewed for necessity. Public IP Addresses that are not intentionally assigned and controlled present a publicly facing vector for threat actors and significant risk to the tenant.

Audit:

Audit from Azure Portal

1. Open the `All Resources` blade
2. Click on `Add Filter`
3. In the Add Filter window, select the following:
   Filter: `Type`
   Operator: `Equals`
   Value: `Public IP address`
4. Click the `Apply` button
5. For each Public IP address in the list, use Overview (or Properties) to review the `"Associated to:"` field and determine if the associated resource is still relevant to your tenant environment. If the associated resource is relevant, ensure that additional controls exist to mitigate risk (e.g. Firewalls, VPNs, Traffic Filtering, Virtual Gateway Appliances, Web Application Firewalls, etc.) on all subsequently attached resources.

Audit from Azure CLI
List all Public IP addresses:

```
az network public-ip list
```

For each Public IP address in the output, review the `"name"` property and determine if the associated resource is still relevant to your tenant environment. If the associated resource is relevant, ensure that additional controls exist to mitigate risk (e.g. Firewalls, VPNs, Traffic Filtering, Virtual Gateway Appliances, Web Application Firewalls, etc.) on all subsequently attached resources.

Remediation:

Remediation will vary significantly depending on your organization's security requirements for the resources attached to each individual Public IP address.

Default Value:

During Virtual Machine and Application creation, a setting may create and attach a public IP.

References:

1. https://docs.microsoft.com/en-us/cli/azure/network/public-ip?view=azure-cli-latest
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.1 Ensure Network Infrastructure is Up-to-Date Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	●	●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

8.8 Ensure that virtual network flow log retention days is set to greater than or equal to 90 (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that virtual network flow logs are retained for greater than or equal to 90 days.

Rationale:

Virtual network flow logs provide critical visibility into traffic patterns. Logs can be used to check for anomalies and give insight into suspected breaches.

Impact:

- Virtual network flow logs are charged per gigabyte of network flow logs collected and come with a free tier of 5 GB/month per subscription.
- If traffic analytics is enabled with virtual network flow logs, traffic analytics pricing applies at per gigabyte processing rates.
- The storage of logs is charged separately, and the cost will depend on the amount of logs and the retention period.

Audit:

Audit from Azure Portal

1. Go to `Network Watcher`.
2. Under `Logs`, select `Flow logs`.
3. Click `Add filter`.
4. From the `Filter` drop-down menu, select `Flow log type`.
5. From the `Value` drop-down menu, check `Virtual network` only.
6. Click `Apply`.
7. Click the name of a virtual network flow log.
8. Under `Storage Account`, ensure that `Retention days` is set to `0`, `90`, or a number greater than 90. If `Retention days` is set to `0`, the logs are retained indefinitely with no retention policy.
9. Repeat steps 7 and 8 for each virtual network flow log.

Audit from Azure CLI
Run the following command to list network watchers:

```
az network watcher list
```

Run the following command to list the name and retention policy of flow logs in a network watcher:

```
az network watcher flow-log list --location <location> --query
[*].[name,retentionPolicy]
```

For each flow log, ensure that `days` is set to `0`, `90`, or a number greater than 90. If `days` is set to `0`, the logs are retained indefinitely with no retention policy.
Repeat for each network watcher.

Remediation:

Remediate from Azure Portal

1. Go to `Network Watcher`.
2. Under `Logs`, select `Flow logs`.
3. Click `Add filter`.
4. From the `Filter` drop-down menu, select `Flow log type`.
5. From the `Value` drop-down menu, check `Virtual network` only.
6. Click `Apply`.
7. Click the name of a virtual network flow log.
8. Under `Storage Account`, set `Retention days` to `0`, `90`, or a number greater than 90. If `Retention days` is set to `0`, the logs are retained indefinitely with no retention policy.
9. Repeat steps 7 and 8 for each virtual network flow log requiring remediation.

Remediate from Azure CLI
Run the following command update the retention policy for a flow log in a network watcher, setting `retention` to `0`, `90`, or a number greater than 90:

```
az network watcher flow-log update --location <location> --name <flow-log> --
retention <number-of-days>
```

Repeat for each virtual network flow log requiring remediation.

Default Value:

When a virtual network flow log is created using the Azure CLI, retention days is set to 0 by default. When creating via the Azure Portal, retention days must be specified by the creator.

References:

1. https://learn.microsoft.com/en-us/azure/network-watcher/vnet-flow-logs-portal
2. https://learn.microsoft.com/en-us/cli/azure/network/watcher/flow-log

Additional Information:

As network security group flow logs are on the retirement path, Azure recommends migrating to virtual network flow logs.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v8	8.10 Retain Audit Logs Retain audit logs across enterprise assets for a minimum of 90 days.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
		M1047

9 Security Services

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

This section covers security best practice recommendations for products in the Azure Security services category.

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#security

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

9.1 Microsoft Defender for Cloud

This subsection provides guidance on the use of Microsoft Defender for Cloud and associated product plans. This guidance is intended to ensure that—at a minimum—the protective measures offered by these plans are being considered. Organizations may find that they have existing products or services that provide the same utility as some Microsoft Defender for Cloud products. Security and Administrative personnel need to make the determination on their organization's behalf regarding which—if any—of these recommendations are relevant to their organization's needs. In consideration of the above, and because of the potential for increased cost and complexity, please be aware that all Microsoft Defender for Cloud and associated plan recommendations are profiled as "Level 2" recommendations.

9.1.1 Microsoft Cloud Security Posture Management (CSPM)

Microsoft Defender for Cloud offers foundational and advanced Cloud Security Posture Management (CSPM) solutions to protect across multi-cloud and hybrid environments. Both solutions cover PaaS as well as IaaS. CSPM provides reporting functionality on security and regulatory frameworks including NIST 800 series, ISO 27001, PCI-DSS, CIS Benchmarks and Controls, and many more. CSPM also provides the ability to create your own custom framework, but this will require significant work. Regulatory standards are reported in a compliance dashboard which offers a summarized view against deployed standards and presents the ability to download compliance reports in various formats.

CSPM has two types of implementations:

1. Foundational (Free): This implementation is free and enabled by default with a limited set of features including:

- Continuous assessment of the security configuration of cloud resources
- Security recommendations to fix misconfigurations and weaknesses
- Secure score summarizing current overall security posture

2. Full CSPM (Paid): Full CSPM is a paid product offering additional functionality including:

- Identity and role assignments discovery
- Network exposure detection
- Attack path analysis
- Cloud security explorer for risk hunting
- Agentless vulnerability scanning
- Agentless secrets scanning
- Governance rules to drive timely remediation and accountability
- Regulatory compliance and industry best practices
- Data-aware security posture
- Agentless discovery for Kubernetes
- Agentless container vulnerability assessment

It is recommended that for full CSPM a cost review is undertaken particularly if your tenant is heavy on IaaS prior to implementing and matched to security requirements.

9.1.2 Defender Plan: APIs

Defender for APIs in Microsoft Defender for Cloud offers full lifecycle protection, detection, and response coverage for APIs published in Azure API Management. Defender for APIs helps you to gain visibility into business-critical APIs. You can investigate and improve your API security posture, prioritize vulnerability fixes, and quickly detect active real-time threats. Defender for APIs requires additional configuration in the Microsoft API portal.

Note: There is a cost attached to using Defender for API.

9.1.3 Defender Plan: Servers

9.1.3.1 Ensure that Defender for Servers is set to 'On' (Automated)

Profile Applicability:

- Level 2

Description:

The Defender for Servers plan in Microsoft Defender for Cloud reduces security risk by providing actionable recommendations to improve and remediate machine security posture. Defender for Servers also helps to protect machines against real-time security threats and attacks.

Defender for Servers offers two paid plans:

Plan 1

The following components are enabled by default:

- Log Analytics agent (deprecated)
- Endpoint protection

Plan 1 also offers the following components, disabled by default:

- Vulnerability assessment for machines
- Guest Configuration agent (preview)

Plan 2

The following components are enabled by default:

- Log Analytics agent (deprecated)
- Vulnerability assessment for machines
- Endpoint protection
- Agentless scanning for machines

Plan 2 also offers the following components, disabled by default:

- Guest Configuration agent (preview)
- File Integrity Monitoring

Rationale:

Enabling Defender for Servers allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Enabling Defender for Servers in Microsoft Defender for Cloud incurs an additional cost per resource. Refer to https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/ and https://azure.microsoft.com/en-us/pricing/calculator/ to estimate potential costs.

- Plan 1: Subscription only
- Plan 2: Subscription and workspace

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment settings`.
3. Click on a subscription name.
4. Select `Defender plans` in the left pane.
5. Under `Cloud Workload Protection (CWP)`, locate `Servers` in the Plan column, ensure Status is set to `On`.
6. Repeat steps 1-5 for each subscription.

Audit from Azure CLI
Run the following command:

```
az security pricing show -n VirtualMachines --query pricingTier
```

If the tenant is licensed and enabled, the output will indicate `Standard`.

Audit from PowerShell
Run the following command:

```
Get-AzSecurityPricing -Name 'VirtualMachines' |Select-Object Name,PricingTier
```

If the tenant is licensed and enabled, the `-PricingTier` parameter will indicate `Standard`.

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:** 4da35fc9-c9e7-4960-aec9-797fe7d9051d **- Name:** 'Azure Defender for servers should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment settings`.
3. Click on a subscription name.
4. Click `Defender plans` in the left pane.
5. Under `Cloud Workload Protection (CWP)`, locate `Servers` in the Plan column, set Status to `On`.
6. Select `Save`.
7. Repeat steps 1-6 for each subscription requiring remediation.

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n VirtualMachines --tier 'standard'
```

Remediate from PowerShell
Run the following command:

```
Set-AzSecurityPricing -Name 'VirtualMachines' -PricingTier 'Standard'
```

Default Value:

By default, the Defender for Servers plan is disabled.

References:

1. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-overview
2. https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers
3. https://learn.microsoft.com/en-us/rest/api/defenderforcloud/pricings/list
4. https://learn.microsoft.com/en-us/rest/api/defenderforcloud/pricings/update
5. https://learn.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
6. https://learn.microsoft.com/en-us/powershell/module/az.security/set-azsecuritypricing
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security#es-1-use-endpoint-detection-and-response-edr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.3.2 Ensure that 'Vulnerability assessment for machines' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

Enable vulnerability assessment for machines on both Azure and hybrid (Arc enabled) machines.

Rationale:

Vulnerability assessment for machines scans for various security-related configurations and events such as system updates, OS vulnerabilities, and endpoint protection, then produces alerts on threat and vulnerability findings.

Impact:

Microsoft Defender for Servers plan 2 licensing is required, and configuration of Azure Arc introduces complexity beyond this recommendation.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Select a subscription
5. Click on `Settings & monitoring`
6. Ensure that `Vulnerability assessment for machines` is set to `On`

Repeat the above for any additional subscriptions.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Select a subscription
5. Click on `Settings & Monitoring`
6. Set the `Status` of `Vulnerability assessment for machines` to `On`
7. Click `Continue`

Repeat the above for any additional subscriptions.

Default Value:

By default, `Automatic provisioning of monitoring agent` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-va
2. https://msdn.microsoft.com/en-us/library/mt704062.aspx
3. https://msdn.microsoft.com/en-us/library/mt704063.aspx
4. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list
5. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-5-perform-vulnerability-assessments

Additional Information:

While this feature is generally available as of publication, it is not yet available for Azure Government tenants.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

9.1.3.3 Ensure that 'Endpoint protection' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

The Endpoint protection component enables Microsoft Defender for Endpoint (formerly 'Advanced Threat Protection' or 'ATP' or 'WDATP' - see additional info) to communicate with Microsoft Defender for Cloud.

IMPORTANT: When enabling integration between DfE & DfC it needs to be taken into account that this will have some side effects that may be undesirable.

1. For server 2019 & above if defender is installed (default for these server SKUs) this will trigger a deployment of the new unified agent and link to any of the extended configuration in the Defender portal.
2. If the new unified agent is required for server SKUs of Win 2016 or Linux and lower there is additional integration that needs to be switched on and agents need to be aligned.

Rationale:

Microsoft Defender for Endpoint integration brings comprehensive Endpoint Detection and Response (EDR) capabilities within Microsoft Defender for Cloud. This integration helps to spot abnormalities, as well as detect and respond to advanced attacks on endpoints monitored by Microsoft Defender for Cloud.

MDE works only with Standard Tier subscriptions.

Impact:

Endpoint protection requires licensing and is included in these plans:

- Defender for Servers plan 1
- Defender for Servers plan 2

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the subscription name.
5. Click `Settings & monitoring`.
6. Ensure the `Status` for `Endpoint protection` is set to `On`.

Audit from Azure CLI

Ensure the output of the below command is `True`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/settings?api-version=2021-06-01' | jq '.|.value[] |
select(.name=="WDATP")'|jq '.properties.enabled'
```

Audit from PowerShell

Run the following commands to login and audit this check

```
Connect-AzAccount
Set-AzContext -Subscription <subscriptionID>
Get-AzSecuritySetting | Select-Object name,enabled |where-object {$_.name -eq
"WDATP"}
```

PowerShell Output - Non-Compliant

```
Name  Enabled
----  -------
WDATP    False
```

PowerShell Output - Compliant

```
Name  Enabled
----  -------
WDATP    True
```

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the subscription name.
5. Click `Settings & monitoring`.
6. Set the `Status` for `Endpoint protection` to `On`.
7. Click `Continue`.

Remediate from Azure CLI

Use the below command to enable Standard pricing tier for Storage Accounts

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/settings/WDATP?api-version=2021-06-01 -d@"input.json"'
```

Where input.json contains the Request body json data as mentioned below.

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/settings/
WDATP",
  "kind": "DataExportSettings",
  "type": "Microsoft.Security/settings",
  "properties": {
    "enabled": true
  }
}
```

Default Value:

By default, Endpoint protection is `off`.

References:

1. https://docs.microsoft.com/en-in/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/update
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security#es-1-use-endpoint-detection-and-response-edr
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security#es-2-use-modern-anti-malware-software

Additional Information:

IMPORTANT: When enabling integration between DfE & DfC it needs to be taken into account that this will have some side effects that may be undesirable.

1. For server 2019 & above if defender is installed (default for these server SKUs) this will trigger a deployment of the new unified agent and link to any of the extended configuration in the Defender portal.
2. If the new unified agent is required for server SKUs of Win 2016 or Linux and lower there is additional integration that needs to be switched on and agents need to be aligned.

NOTE: "Microsoft Defender for Endpoint (MDE)" was formerly known as "Windows Defender Advanced Threat Protection (WDATP)." There are a number of places (e.g. Azure CLI) where the "WDATP" acronym is still used within Azure.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	13.2 Deploy a Host-Based Intrusion Detection Solution Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1562	TA0005	

9.1.3.4 Ensure that 'Agentless scanning for machines' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

Using disk snapshots, the agentless scanner scans for installed software, vulnerabilities, and plain text secrets.

Rationale:

The Microsoft Defender for Cloud agentless machine scanner provides threat detection, vulnerability detection, and discovery of sensitive information.

Impact:

Agentless scanning for machines requires licensing and is included in these plans:

- Defender CSPM
- Defender for Servers plan 2

Audit:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `Agentless scanning for machines`
6. Ensure that `On` is selected

Repeat the above for any additional subscriptions.

Remediation:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `Agentless scanning for machines`
6. Select `On`

7. Click `Continue` in the top left

Repeat the above for any additional subscriptions.

Default Value:

By default, Agentless scanning for machines is `off`.

References:

1. https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-data-collection
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification
3. https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

9.1.3.5 Ensure that 'File Integrity Monitoring' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

File Integrity Monitoring (FIM) is a feature that monitors critical system files in Windows or Linux for potential signs of attack or compromise.

Rationale:

FIM provides a detection mechanism for compromised files. When FIM is enabled, critical system files are monitored for changes that might indicate a threat actor is attempting to modify system files for lateral compromise within a host operating system.

Impact:

File Integrity Monitoring requires licensing and is included in these plans:

- Defender for Servers plan 2

Audit:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `File Integrity Monitoring`
6. Ensure that `On` is selected

Repeat the above for any additional subscriptions.

Remediation:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `File Integrity Monitoring`
6. Select `On`
7. Click `Continue` in the top left

Repeat the above for any additional subscriptions.

Default Value:

By default, File Integrity Monitoring is `Off`.

References:

1. https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification
3. https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-enable-defender-endpoint

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

9.1.4 Defender Plan: Containers

9.1.4.1 Ensure That Microsoft Defender for Containers Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Microsoft Defender for Containers helps improve, monitor, and maintain the security of containerized assets—including Kubernetes clusters, nodes, workloads, container registries, and images—across multi-cloud and on-premises environments.

By default, when enabling the plan through the Azure Portal, Microsoft Defender for Containers automatically configures the following components:

- **Agentless scanning for machines**
- **Defender sensor** for runtime protection
- **Azure Policy** for enforcing security best practices
- **K8S API access** for monitoring and threat detection
- **Registry access** for vulnerability assessment

Note: Microsoft Defender for Container Registries ('ContainerRegistry') is deprecated and has been replaced by Microsoft Defender for Containers ('Containers').

Rationale:

Enabling Microsoft Defender for Containers enhances defense-in-depth by providing advanced threat detection, vulnerability assessment, and security monitoring for containerized environments, leveraging insights from the Microsoft Security Response Center (MSRC).

Impact:

Microsoft Defender for Containers incurs a charge per vCore. Refer to https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/ and https://azure.microsoft.com/en-us/pricing/calculator/ to estimate potential costs.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, click `Environment settings`.
3. Click the name of a subscription.
4. Under `Settings`, click `Defender plans`.
5. Under `Cloud Workload Protection (CWP)`, in the row for `Containers`, ensure that the `Status` is set to `On` and `Monitoring coverage` displays `Full`.
6. Repeat steps 1-5 for each subscription.

Audit from Azure CLI
For Microsoft Defender for Container Registries (deprecated), run the following command:

```
az security pricing show --name "ContainerRegistry" --query pricingTier
```

Ensure that the command returns `Standard`.
For Microsoft Defender for Containers, run the following command:

```
az security pricing show --name "Containers" --query
[pricingTier,extensions[*].[name,isEnabled]]
```

Ensure that the command returns `Standard`, and that each of the extensions (ContainerRegistriesVulnerabilityAssessments, AgentlessDiscoveryForKubernetes, AgentlessVmScanning, ContainerSensor) returns `True`.
Repeat for each subscription.
Audit from PowerShell
For Microsoft Defender for Container Registries (deprecated), run the following command:

```
Get-AzSecurityPricing -Name 'ContainerRegistry' | Select-Object
Name,PricingTier
```

Ensure the command returns `PricingTier Standard`.
For Microsoft Defender for Containers, run the following command:

```
Get-AzSecurityPricing -Name 'Containers'
```

Ensure that `PricingTier` is set to `Standard`, and that each of the extensions (ContainerRegistriesVulnerabilityAssessments, AgentlessDiscoveryForKubernetes, AgentlessVmScanning, ContainerSensor) has `isEnabled` set to `True`.
Repeat for each subscription.
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:** 1c988dd6-ade4-430f-a608-2a3e5b0a6d38 **- Name:** 'Microsoft Defender for Containers should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, click `Environment settings`.
3. Click the name of a subscription.
4. Under `Settings`, click `Defender plans`.
5. Under `Cloud Workload Protection (CWP)`, in the row for `Containers`, click `On` in the `Status` column.
6. If `Monitoring coverage` displays `Partial`, click `Settings` under `Partial`.

7. Set the status of each of the components to `On`.
8. Click `Continue`.
9. Click `Save`.
10. Repeat steps 1-9 for each subscription.

Remediate from Azure CLI

Note: Microsoft Defender for Container Registries ('ContainerRegistry') is deprecated and has been replaced by Microsoft Defender for Containers ('Containers').
Run the below command to enable the Microsoft Defender for Containers plan and its components:

```
az security pricing create -n 'Containers' --tier 'standard' --extensions
name=ContainerRegistriesVulnerabilityAssessments isEnabled=True --extensions
name=AgentlessDiscoveryForKubernetes isEnabled=True --extensions
name=AgentlessVmScanning isEnabled=True --extensions name=ContainerSensor
isEnabled=True
```

Remediate from PowerShell

Note: Microsoft Defender for Container Registries ('ContainerRegistry') is deprecated and has been replaced by Microsoft Defender for Containers ('Containers').
Run the below command to enable the Microsoft Defender for Containers plan and its components:

```
Set-AzSecurityPricing -Name 'Containers' -PricingTier 'Standard' -Extension
'[{"name":"ContainerRegistriesVulnerabilityAssessments","isEnabled":"True"},{
"name":"AgentlessDiscoveryForKubernetes","isEnabled":"True"},{"name":"Agentle
ssVmScanning","isEnabled":"True"},{"name":"ContainerSensor","isEnabled":"True
"}]'
```

Default Value:

The Microsoft Defender for Containers plan is disabled by default.

References:

1. https://learn.microsoft.com/en-us/cli/azure/security/pricing
2. https://learn.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
3. https://learn.microsoft.com/en-us/powershell/module/az.security/set-azsecuritypricing
4. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction
5. https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-enable-containers-azure
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

Additional Information:

The Azure Policy 'Microsoft Defender for Containers should be enabled' checks only that the `pricingTier` for `Containers` is set to `Standard`. It does not check the status of the plan's components.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.5 Defender Plan: Storage

9.1.5.1 Ensure That Microsoft Defender for Storage Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Storage enables threat detection for Storage, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Storage allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Storage incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Ensure `Status` is set to `On` for `Storage`.

Audit from Azure CLI
Ensure the output of the below command is Standard

```
az security pricing show -n StorageAccounts
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'StorageAccounts' | Select-Object
Name,PricingTier
```

Ensure output for `Name PricingTier` is `StorageAccounts Standard`
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:** 640d2586-54d2-465f-877f-9ffc1d2109f4 **- Name:** 'Microsoft Defender for Storage should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Set `Status` to `On` for `Storage`.
6. Select `Save`.

Remediate from Azure CLI

Ensure the output of the below command is Standard

```
az security pricing create -n StorageAccounts --tier 'standard'
```

Remediate from PowerShell

```
Set-AzSecurityPricing -Name 'StorageAccounts' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.6 Defender Plan: App Service

9.1.6.1 Ensure That Microsoft Defender for App Services Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for App Service enables threat detection for App Service, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for App Service allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for App Service incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Select `Defender plans`
5. Ensure Status is `On` for `App Service`

Audit from Azure CLI
Run the following command:

```
az security pricing show -n AppServices
```

Ensure `-PricingTier` is set to `Standard`

Audit from PowerShell
Run the following command:

```
Get-AzSecurityPricing -Name 'AppServices' |Select-Object Name,PricingTier
```

Ensure the `-PricingTier` is set to `Standard`

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:** 2913021d-f2fd-4f3d-b958-22354e2bdbcb **- Name:** 'Azure Defender for App Service should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Select `Defender plans`
5. Set `App Service` Status to `On`
6. Select `Save`

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n Appservices --tier 'standard'
```

Remediate from PowerShell
Run the following command:

```
Set-AzSecurityPricing -Name "AppServices" -PricingTier "Standard"
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.7 Defender Plan: Databases

9.1.7.1 Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Microsoft Defender for Azure Cosmos DB scans all incoming network requests for threats to your Azure Cosmos DB resources.

Rationale:

In scanning Azure Cosmos DB requests within a subscription, requests are compared to a heuristic list of potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.

Impact:

Enabling Microsoft Defender for Azure Cosmos DB requires enabling Microsoft Defender for your subscription. Both will incur additional charges.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. On the `Database` row click on `Select types >`.
6. Ensure the toggle switch next to `Azure Cosmos DB` is set to `On`.

Audit from Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n CosmosDbs --query pricingTier
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'CosmosDbs' | Select-Object Name,PricingTier
```

Ensure output of `-PricingTier` is `Standard`

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:** adbe85b5-83e6-4350-ab58-bf3a4f736e5e **- Name:** 'Microsoft Defender for Azure Cosmos DB should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. On the `Database` row click on `Select types >`.
6. Set the toggle switch next to `Azure Cosmos DB` to `On`.
7. Click `Continue`.
8. Click `Save`.

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n 'CosmosDbs' --tier 'standard'
```

Remediate from PowerShell
Use the below command to enable Standard pricing tier for Azure Cosmos DB

```
Set-AzSecurityPricing -Name 'CosmosDbs' -PricingTier 'Standard
```

Default Value:

By default, Microsoft Defender for Azure Cosmos DB is not enabled.

References:

1. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
2. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
3. https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview
4. https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cosmos-db-security-baseline
5. https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-enable-database-protections
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.7.2 Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Open-source relational databases enables threat detection for Open-source relational databases, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Open-source relational databases allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Open-source relational databases incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the toggle switch next to `Open-source relational databases` is set to `On`.

Audit from Azure CLI
Run the following command:

```
az security pricing show -n OpenSourceRelationalDatabases --query pricingTier
```

Audit from PowerShell

```
Get-AzSecurityPricing | Where-Object {$_.Name -eq
'OpenSourceRelationalDatabases'} | Select-Object Name, PricingTier
```

Ensure output for `Name PricingTier` is `OpenSourceRelationalDatabases Standard`

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:** 0a9fbe0d-c5c4-4da8-87d8-f4fd77338835 **- Name:** 'Azure Defender for open-source relational databases should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Set the toggle switch next to `Open-source relational databases` to `On`.
7. Select `Continue`.
8. Select `Save`.

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n 'OpenSourceRelationalDatabases' --tier
'standard'
```

Remediate from PowerShell
Use the below command to enable Standard pricing tier for Open-source relational databases

```
set-azsecuritypricing -name "OpenSourceRelationalDatabases" -pricingtier
"Standard"
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
3. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.7.3 Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Azure SQL Databases enables threat detection for Managed Instance Azure SQL databases, providing threat intelligence, anomaly detection, and behavior analytics in Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Azure SQL Databases allows for greater defense-in-depth, includes functionality for discovering and classifying sensitive data, surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database.

Impact:

Turning on Microsoft Defender for Azure SQL Databases incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the toggle switch next to `Azure SQL Databases` is set to `On`.

Audit from Azure CLI
Run the following command:

```
az security pricing show -n SqlServers
```

Ensure `-PricingTier` is set to `Standard`

Audit from PowerShell
Run the following command:

```
Get-AzSecurityPricing -Name 'SqlServers' | Select-Object Name,PricingTier
```

Ensure the `-PricingTier` is set to `Standard`

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:** 7fe3b40f-802b-4cdd-8bd4-fd799c948cc2 **- Name:** 'Azure Defender for Azure SQL Database servers should be enabled'
- **Policy ID:** abfb7388-5bf4-4ad7-ba99-2cd2f41cebb9 **- Name:** 'Azure Defender for SQL should be enabled for unprotected SQL Managed Instances'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Set the toggle switch next to `Azure SQL Databases` to `On`.
7. Select `Continue`.
8. Select `Save`.

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n SqlServers --tier 'standard'
```

Remediate from PowerShell
Run the following command:

```
Set-AzSecurityPricing -Name 'SqlServers' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.7.4 Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for SQL servers on machines enables threat detection for SQL servers on machines, providing threat intelligence, anomaly detection, and behavior analytics in Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for SQL servers on machines allows for greater defense-in-depth, functionality for discovering and classifying sensitive data, surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database.

Impact:

Turning on Microsoft Defender for SQL servers on machines incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the toggle switch next to `SQL servers on machines` is set to `On`.

Audit from Azure CLI
Ensure Defender for SQL is licensed with the following command:

```
az security pricing show -n SqlServerVirtualMachines
```

Ensure the 'PricingTier' is set to 'Standard'
Audit from PowerShell
Run the following command:

```
Get-AzSecurityPricing -Name 'SqlServerVirtualMachines' | Select-Object
Name,PricingTier
```

Ensure the 'PricingTier' is set to 'Standard'

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:** 6581d072-105e-4418-827f-bd446d56421b **- Name:** 'Azure Defender for SQL servers on machines should be enabled'
- **Policy ID:** abfb4388-5bf4-4ad7-ba82-2cd2f41ceae9 **- Name:** 'Azure Defender for SQL should be enabled for unprotected Azure SQL servers'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Set the toggle switch next to `SQL servers on machines` to `On`.
7. Select `Continue`.
8. Select `Save`.

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n SqlServerVirtualMachines --tier 'standard'
```

Remediate from PowerShell
Run the following command:

```
Set-AzSecurityPricing -Name 'SqlServerVirtualMachines' -PricingTier
'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/defender-for-sql-usage
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data

6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.8 Defender Plan: Key Vault

9.1.8.1 Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Key Vault enables threat detection for Key Vault, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Key Vault allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Key Vault incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Ensure `Status` is set to `On` for `Key Vault`.

Audit from Azure CLI
Ensure the output of the below command is Standard

```
az security pricing show -n 'KeyVaults' --query 'pricingTier'
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'KeyVaults' | Select-Object Name,PricingTier
```

Ensure output for `PricingTier` is `Standard`
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:** 0e6763cc-5078-4e64-889d-ff4d9a839047 **- Name:** 'Azure Defender for Key Vault should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Select `On` under `Status` for `Key Vault`.
6. Select `Save`.

Remediate from Azure CLI
Enable Standard pricing tier for Key Vault:

```
az security pricing create -n 'KeyVaults' --tier 'Standard'
```

Remediate from PowerShell
Enable Standard pricing tier for Key Vault:

```
Set-AzSecurityPricing -Name 'KeyVaults' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.9 Defender Plan: Resource Manager

9.1.9.1 Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Microsoft Defender for Resource Manager scans incoming administrative requests to change your infrastructure from both CLI and the Azure portal.

Rationale:

Scanning resource requests lets you be alerted every time there is suspicious activity in order to prevent a security threat from being introduced.

Impact:

Enabling Microsoft Defender for Resource Manager requires enabling Microsoft Defender for your subscription. Both will incur additional charges.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Ensure `Status` is set to `On` for `Resource Manager`.

Audit from Azure CLI
Ensure the output of the below command is Standard

```
az security pricing show -n 'Arm' --query 'pricingTier'
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'Arm' | Select-Object Name,PricingTier
```

Ensure the output of `PricingTier` is `Standard`
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:** c3d20c29-b36d-48fe-808b-99a87530ad99 **- Name:** 'Azure Defender for Resource Manager should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Select `On` under `Status` for `Resource Manager`.
6. Select `Save.

Remediate from Azure CLI
Use the below command to enable Standard pricing tier for Defender for Resource Manager

```
az security pricing create -n 'Arm' --tier 'Standard'
```

Remediate from PowerShell
Use the below command to enable Standard pricing tier for Defender for Resource Manager

```
Set-AzSecurityPricing -Name 'Arm' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender for Resource Manager is not enabled.

References:

1. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
2. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-resource-manager-introduction
3. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
4. https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.1.10 Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that the latest OS patches for all virtual machines are applied.

Rationale:

Windows and Linux virtual machines should be kept updated to:

- Address a specific bug or flaw
- Improve an OS or application's general stability
- Fix a security vulnerability

Microsoft Defender for Cloud retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on which service is configured on a Windows VM. The security center also checks for the latest updates in Linux systems. If a VM is missing a system update, the security center will recommend system updates be applied.

Impact:

Running Microsoft Defender for Cloud incurs additional charges for each resource monitored. Please see attached reference for exact charges per hour.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Then the `Recommendations` blade
4. Ensure that there are no recommendations for `System updates should be installed on your machines (powered by Update Center)`

Alternatively, you can employ your own patch assessment and management tool to periodically assess, report and install the required security patches for your OS.

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:** f85bf3e0-d513-442e-89c3-1784ad63382b **- Name:** 'System updates should be installed on your machines (powered by Update Center)'
- **Policy ID:** bd876905-5b84-4f73-ab2d-2e7a7c4568d9 **- Name:** 'Machines should be configured to periodically check for missing system updates'

Remediation:

Follow Microsoft Azure documentation to apply security patches from the security center. Alternatively, you can employ your own patch assessment and management tool to periodically assess, report, and install the required security patches for your OS.

Default Value:

By default, patches are not automatically deployed.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities
2. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
3. https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1068	TA0004	M1051

9.1.11 Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

The Microsoft Cloud Security Benchmark (or "MCSB") is an Azure Policy Initiative containing many security policies to evaluate resource configuration against best practice recommendations. If a policy in the MCSB is set with effect type `Disabled`, it is not evaluated and may prevent administrators from being informed of valuable security recommendations.

Rationale:

A security policy defines the desired configuration of resources in your environment and helps ensure compliance with company or regulatory security requirements. The MCSB Policy Initiative a set of security recommendations based on best practices and is associated with every subscription by default. When a policy "Effect" is set to `Audit`, policies in the MCSB ensure that Defender for Cloud evaluates relevant resources for supported recommendations. To ensure that policies within the MCSB are not being missed when the Policy Initiative is evaluated, none of the policies should have an Effect of `Disabled`.

Impact:

Policies within the MCSB default to an effect of `Audit` and will evaluate—but not enforce—policy recommendations. Ensuring these policies are set to `Audit` simply ensures that the evaluation occurs to allow administrators to understand where an improvement may be possible. Administrators will need to determine if the recommendations are relevant and desirable for their environment, then manually take action to resolve the status if desired.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment settings`.
4. Click on the appropriate Management Group or Subscription.
5. Click on `Security policies` in the left column.
6. Click on `Microsoft cloud security benchmark`.
7. Click `Add filter` and select `Effect`.
8. Check the `Disabled` box to search for all disabled policies.
9. Click `Apply`.
10. Ensure that no policies are displayed, signifying that there are no disabled policies.
11. Repeat steps 1-10 for each Management Group or Subscription.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment settings`.
4. Click on the appropriate Management Group or Subscription.
5. Click on `Security policies` in the left column.
6. Click on `Microsoft cloud security benchmark`
7. Click `Add Filter` and select `Effect`
8. Check the `Disabled` box to search for all disabled policies
9. Click `Apply`
10. Click the blue ellipsis `...` to the right of a policy name.
11. Click `Manage effect and parameters`.
12. Under `Policy effect`, select the radio button next to `Audit`.
13. Click `Save`.
14. Click `Refresh`.
15. Repeat steps 10-14 until all disabled policies are updated.
16. Repeat steps 1-15 for each Management Group or Subscription requiring remediation.

Default Value:

By default, the MCSB policy initiative is assigned on all subscriptions, and **most** policies will have an effect of `Audit`. Some policies will have a default effect of `Disabled`.

References:

1. https://learn.microsoft.com/en-in/azure/defender-for-cloud/security-policy-concept
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
3. https://learn.microsoft.com/en-us/azure/defender-for-cloud/implement-security-recommendations
4. https://learn.microsoft.com/en-us/rest/api/policy/policy-assignments/get
5. https://learn.microsoft.com/en-us/rest/api/policy/policy-assignments/create
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-7-define-and-implement-logging-threat-detection-and-incident-response-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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.	●	●	●
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

9.1.12 Ensure That 'All users with the following roles' is set to 'Owner' (Automated)

Profile Applicability:

- Level 1

Description:

Enable security alert emails to subscription owners.

Rationale:

Enabling security alert emails to subscription owners ensures that they receive security alert emails from Microsoft. This ensures that they are aware of any potential security issues and can mitigate the risk in a timely fashion.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on `Email notifications`
6. Ensure that `All users with the following roles` is set to `Owner`

Audit from Azure CLI
Ensure the command below returns state of `On` and that `Owner` appears in roles.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview'| jq '.[] |
select(.name=="default").properties.notificationsByRole'
```

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on `Email notifications`
6. In the drop down of the `All users with the following roles` field select `Owner`
7. Click `Save`

Remediate from Azure CLI

Use the below command to set `Send email also to subscription owners` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the data below, replacing `validEmailAddress` with a single email address or multiple comma-separated email addresses:

```
    {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
      "name": "default1",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "alertNotifications": "On",
        "alertsToAdmins": "On",
       "notificationsByRole": "Owner"
      }
    }
```

Default Value:

By default, `Owner` is selected

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

Additional Information:

Excluding any entries in the input.json properties block disables the specific setting by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.2 Establish and Maintain Contact Information for Reporting Security Incidents Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	●	●	●
v7	19.5 Maintain Contact Information For Reporting Security Incidents Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	●	●	●

9.1.13 Ensure 'Additional email addresses' is Configured with a Security Contact Email (Automated)

Profile Applicability:

- Level 1

Description:

Microsoft Defender for Cloud emails the subscription owners whenever a high-severity alert is triggered for their subscription. You should provide a security contact email address as an additional email address.

Rationale:

Microsoft Defender for Cloud emails the Subscription Owner to notify them about security alerts. Adding your Security Contact's email address to the 'Additional email addresses' field ensures that your organization's Security Team is included in these alerts. This ensures that the proper people are aware of any potential compromise in order to mitigate the risk in a timely fashion.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the appropriate Management Group, Subscription, or Workspace.
5. Click on `Email notifications`.
6. Ensure that a valid security contact email address is listed in the `Additional email addresses` field.

Audit from Azure CLI
Ensure the output of the below command is not empty and is set with appropriate email ids:

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview' | jq '.|.[] |
select(.name=="default")'|jq '.properties.emails'
```

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:** 4f4f78b8-e367-4b10-a341-d9a4ad5cf1c7 **- Name:** 'Subscriptions should have a contact email address for security issues'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the appropriate Management Group, Subscription, or Workspace.
5. Click on `Email notifications`.
6. Enter a valid security contact email address (or multiple addresses separated by commas) in the `Additional email addresses` field.
7. Click `Save`.

Remediate from Azure CLI
Use the below command to set `Security contact emails` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default?api-version=2020-01-01-preview -d@"input.json"'
```

Where `input.json` contains the data below, replacing `validEmailAddress` with a single email address or multiple comma-separated email addresses:

```
    {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default",
      "name": "default",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "alertNotifications": "On",
        "alertsToAdmins": "On"
      }
    }
```

Default Value:

By default, there are no additional email addresses entered.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

Additional Information:

Excluding any entries in the input.json properties block disables the specific setting by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.2 Establish and Maintain Contact Information for Reporting Security Incidents Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	●	●	●
v7	19.5 Maintain Contact Information For Reporting Security Incidents Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	●	●	●

9.1.14 Ensure that 'Notify about alerts with the following severity (or higher)' is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Enables emailing security alerts to the subscription owner or other designated security contact.

Rationale:

Enabling security alert emails ensures that security alert emails are sent by Microsoft. This ensures that the right people are aware of any potential security issues and can mitigate the risk.

Impact:

Enabling security alert emails can cause alert fatigue, increasing the risk of missing important alerts. Select an appropriate severity level to manage notifications. Azure aims to reduce alert fatigue by limiting the daily email volume per severity level. Learn more: https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications#email-frequency.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment settings`.
4. Click on the appropriate Subscription.
5. Click on `Email notifications`.
6. Under `Notification types`, ensure that the box next to `Notify about alerts with the following severity (or higher)` is checked, and an appropriate severity level is selected.
7. Repeat steps 1-6 for each Subscription.

Audit from Azure CLI
Including a Subscription ID at the `$0` in `/subscriptions/$0/providers`, ensure the below command returns `"state": "On"`, and that `"minimalSeverity"` is set to an appropriate severity level:

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview' | jq '.|.[] |
select(.name=="default")'|jq '.properties.alertNotifications'
```

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:** 6e2593d9-add6-4083-9c9b-4b7d2188c899 **- Name:** 'Email notification for high severity alerts should be enabled'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment settings`.
4. Click on the appropriate Subscription.
5. Click on `Email notifications`.
6. Under `Notification types`, check box next to `Notify about alerts with the following severity (or higher)` and select an appropriate severity level from the drop-down menu.
7. Click `Save`.
8. Repeat steps 1-7 for each Subscription requiring remediation.

Remediate from Azure CLI
Use the below command to enable `Send email notification for high severity alerts`:

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<$0>/providers/Microsoft.Security/
securityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the data below, replacing `validEmailAddress` with a single email address or multiple comma-separated email addresses: *[next page]*

```
{
  "id":
"/subscriptions/<subscriptionId>/providers/Microsoft.Security/securityContact
s/default",
  "name": "default",
  "type": "Microsoft.Security/securityContacts",
  "properties": {
  "email": "<validEmailAddress>",
  "alertNotifications": "On",
  "alertsToAdmins": "On"
  }
}
```

Default Value:

By default, subscription owners receive email notifications for high-severity alerts.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

Additional Information:

Excluding any entries in the `input.json` properties block disables the specific setting by default. This recommendation has been updated to reflect recent changes to Microsoft REST APIs for getting and updating security contact information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.11 Tune Security Event Alerting Thresholds Tune security event alerting thresholds monthly, or more frequently.			●
v7	6.8 Regularly Tune SIEM On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			●

9.1.15 Ensure that 'Notify about attack paths with the following risk level (or higher)' is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Enables emailing attack paths to the subscription owner or other designated security contact.

Rationale:

Enabling attack path emails ensures that attack path emails are sent by Microsoft. This ensures that the right people are aware of any potential security issues and can mitigate the risk.

Impact:

Enabling attack path emails can cause alert fatigue, increasing the risk of missing important alerts. Select an appropriate risk level to manage notifications. Azure aims to reduce alert fatigue by limiting the daily email volume per risk level. Learn more: https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications#email-frequency.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment settings`.
4. Click on the appropriate Subscription.
5. Click on `Email notifications`.
6. Under Notification types, ensure that the box next to `Notify about attack paths with the following risk level (or higher)` is checked, and an appropriate risk level is selected.
7. Repeat steps 1-6 for each Subscription.

Audit from Azure CLI

Including a Subscription ID at the `$0` in `/subscriptions/$0/providers`, ensure the below command returns `"sourceType": "AttackPath"`, and that `"minimalRiskLevel"` is set to an appropriate risk level:

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2023-12-01-preview' | jq '.|.[]'
```

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment settings`.
4. Click on the appropriate Subscription.
5. Click on `Email notifications`.
6. Under Notification types, check the box next to `Notify about attack paths with the following risk level (or higher)`, and select an appropriate risk level from the drop-down menu.
7. Repeat steps 1-6 for each Subscription.

References:

1. https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications
2. https://learn.microsoft.com/en-us/azure/defender-for-cloud/how-to-manage-attack-path
3. https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-attack-path

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.11 Tune Security Event Alerting Thresholds Tune security event alerting thresholds monthly, or more frequently.			●
v7	6.8 Regularly Tune SIEM On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			●

9.1.16 Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled (Manual)

Profile Applicability:

- Level 2

Description:

An organization's attack surface is the collection of assets with a public network identifier or URI that an external threat actor can see or access from outside your cloud. It is the set of points on the boundary of a system, a system element, system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, system component, or environment. The larger the attack surface, the harder it is to protect.

This tool can be configured to scan your organization's online infrastructure such as specified domains, hosts, CIDR blocks, and SSL certificates, and store them in an Inventory. Inventory items can be added, reviewed, approved, and removed, and may contain enrichments ("insights") and additional information collected from the tool's different scan engines and open-source intelligence sources.

A Defender EASM workspace will generate an Inventory of publicly exposed assets by crawling and scanning the internet using *Seeds* you provide when setting up the tool. Seeds can be FQDNs, IP CIDR blocks, and WHOIS records.

Defender EASM will generate Insights within 24-48 hours after Seeds are provided, and these insights include vulnerability data (CVEs), ports and protocols, and weak or expired SSL certificates that could be used by an attacker for reconnaissance or exploitation.

Results are classified High/Medium/Low and some of them include proposed mitigations.

Rationale:

This tool can monitor the externally exposed resources of an organization, provide valuable insights, and export these findings in a variety of formats (including CSV) for use in vulnerability management operations and red/purple team exercises.

Impact:

Microsoft Defender EASM workspaces are currently available as Azure Resources with a 30-day free trial period but can quickly accrue significant charges. The costs are calculated daily as (Number of "billable" inventory items) x (item cost per day; approximately: $0.017).

Estimated cost is not provided within the tool, and users are strongly advised to contact their Microsoft sales representative for pricing and set a calendar reminder for the end of the trial period.

For an EASM workspace having an Inventory of 5k-10k billable items (IP addresses, hostnames, SSL certificates, etc) a typical cost might be approximately $85-170 per day or $2500-5000 USD/month at the time of publication.

If the workspace is deleted by the last day of a free trial period, no charges are billed.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender EASM`.
2. Ensure that at least one Microsoft Defender EASM workspace is listed.
3. Click the name of a workspace.
4. Ensure the workspace is configured appropriately for your environment and organization.
5. Repeat steps 3-4 for each workspace.

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender EASM`.
2. Click `+ Create`.
3. Under `Project details`, select a subscription.
4. Select or create a resource group.
5. Under `Instance details`, enter a name for the workspace.
6. Select a region.
7. Click `Review + create`.
8. Click `Create`.
9. Once the deployment has completed, go to `Microsoft Defender EASM`.
10. Click the workspace name.
11. Configure the workspace appropriately for your environment and organization.

Default Value:

Microsoft Defender EASM is an optional, paid Azure Resource that must be created and configured inside a Subscription and Resource Group.

References:

1. https://learn.microsoft.com/en-us/azure/external-attack-surface-management/
2. https://learn.microsoft.com/en-us/azure/external-attack-surface-management/deploying-the-defender-easm-azure-resource
3. https://www.microsoft.com/en-us/security/blog/2022/08/02/microsoft-announces-new-solutions-for-threat-intelligence-and-attack-surface-management/

Additional Information:

Microsoft added its Defender for External Attack Surface management (EASM) offering to Azure following its 2022 acquisition of EASM SaaS tool company RiskIQ.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

9.1.17 [LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

[**NOTE:** As of August 1, 2023 customers with an existing subscription to Defender for DNS can continue to use the service, but new subscribers will receive alerts about suspicious DNS activity as part of Defender for Servers P2.]

Microsoft Defender for DNS scans all network traffic exiting from within a subscription.

Rationale:

DNS lookups within a subscription are scanned and compared to a dynamic list of websites that might be potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.

Impact:

Enabling Microsoft Defender for DNS requires enabling Microsoft Defender for your subscription. Both will incur additional charges, with Defender for DNS being a small amount per million queries.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Select the `Defender plans` blade
5. Ensure `Status` is set to `On` for `DNS`.

Audit from Azure CLI
Ensure the output of the below command is Standard

```
az security pricing show -n 'DNS' --query 'PricingTier'
```

Audit from PowerShell

```
Get-AzSecurityPricing --Name 'DNS' | Select-Object Name,PricingTier
```

Ensure output of `PricingTier` is `Standard`

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:** bdc59948-5574-49b3-bb91-76b7c986428d **- Name:** 'Azure Defender for DNS should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Select `On` under `Status` for `DNS`.
6. Select `Save`.

Remediate from Azure CLI
Enable Standard pricing tier for DNS:

```
az security pricing create -n 'DNS' --tier 'Standard'
```

Remediate from PowerShell
Enable Standard pricing tier for DNS:

```
Set-AzSecurityPricing -Name 'DNS' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender for DNS is not enabled.

References:

1. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
2. https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/dns-security-baseline
3. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-dns-alerts
4. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
5. https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview
6. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-10-ensure-domain-name-system-dns-security
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

Additional Information:

[**NOTE:** As of August 1, 2023 customers with an existing subscription to Defender for DNS can continue to use the service, but new subscribers will receive alerts about suspicious DNS activity as part of Defender for Servers P2.]

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.9 Configure Trusted DNS Servers on Enterprise Assets Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		●	●
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●
v7	7.6 Log all URL requests Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1016, M1050

9.2 Microsoft Defender for IoT

9.2.1 Ensure That Microsoft Defender for IoT Hub Is Set To 'On' (Manual)

Profile Applicability:

- Level 2

Description:

Microsoft Defender for IoT acts as a central security hub for IoT devices within your organization.

Rationale:

IoT devices are very rarely patched and can be potential attack vectors for enterprise networks. Updating their network configuration to use a central security hub allows for detection of these breaches.

Impact:

Enabling Microsoft Defender for IoT will incur additional charges dependent on the level of usage.

Audit:

Audit from Azure Portal

1. Go to `IoT Hub`.
2. Select an `IoT Hub` to validate.
3. Select `Overview` in `Defender for IoT`.
4. The Threat prevention and Threat detection screen will appear, if `Defender for IoT` is Enabled.

Remediation:

Remediate from Azure Portal

1. Go to `IoT Hub`.
2. Select an `IoT Hub` to validate.
3. Select `Overview` in `Defender for IoT`.
4. Click on `Secure your IoT solution`, and complete the onboarding.

Default Value:

By default, Microsoft Defender for IoT is not enabled.

References:

1. https://azure.microsoft.com/en-us/services/iot-defender/#overview

2. https://docs.microsoft.com/en-us/azure/defender-for-iot/
3. https://azure.microsoft.com/en-us/pricing/details/iot-defender/
4. https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/defender-for-iot-security-baseline
5. https://docs.microsoft.com/en-us/cli/azure/iot?view=azure-cli-latest
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities
7. https://learn.microsoft.com/en-us/azure/defender-for-iot/device-builders/quickstart-onboard-iot-hub

Additional Information:

There are additional configurations for Microsoft Defender for IoT that allow for types of deployments called hybrid or local. Both run on your physical infrastructure. These are complicated setups and are primarily outside of the scope of a purely Azure benchmark. Please see the references to consider these options for your organization.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

9.3 Key Vault

This section covers security recommendations to follow for the configuration and use of Azure Key Vault.

9.3.1 Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Keys in Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration date) attribute identifies the expiration date on or after which the key MUST NOT be used for encryption of new data, wrapping of new keys, and signing. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration date for all keys to help enforce the key rotation. This ensures that the keys cannot be used beyond their assigned lifetimes.

Impact:

Keys cannot be used beyond their assigned expiration dates respectively. Keys need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that an appropriate `Expiration date` is set for any keys that are `Enabled`.

Audit from Azure CLI

Get a list of all the key vaults in your Azure environment by running the following command:

```
az keyvault list
```

Then for each key vault listed ensure that the output of the below command contains Key ID (kid), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault key list --vault-name <VaultName> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Azure Key vaults:

```
Get-AzKeyVault
```

For each Key vault run the following command to determine which vaults are configured to use RBAC.

```
Get-AzKeyVault -VaultName <VaultName>
```

For each Key vault with the `EnableRbacAuthorizatoin` setting set to `True`, run the following command.

```
Get-AzKeyVaultKey -VaultName <VaultName>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

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:** 152b15f7-8e1f-4c1f-ab71-8c010ba5dbc0 **- Name:** 'Key Vault keys should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that an appropriate `Expiration date` is set for any keys that are `Enabled`.

Remediate from Azure CLI
Update the `Expiration date` for the key using the below command:

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --
expires Y-m-d'T'H:M:S'Z'
```

Note:
To view the expiration date on all keys in a Key Vault using Microsoft API, the "List" Key permission is required.
To update the expiration date for the keys:

1. Go to the Key vault, click on Access Control (IAM).
2. Click on Add role assignment and assign the role of Key Vault Crypto Officer to the appropriate user.

Remediate from PowerShell

```
Set-AzKeyVaultKeyAttribute -VaultName <VaultName> -Name <KeyName> -Expires
<DateTime>
```

Default Value:

By default, keys do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-keys
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyattribute?view=azps-0.10.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1047

9.3.2 Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Keys in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration date) attribute identifies the expiration date on or after which the key MUST NOT be used for a cryptographic operation. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration date for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes.

Impact:

Keys cannot be used beyond their assigned expiration dates respectively. Keys need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that the status of the key is `Enabled`.
4. For each enabled key, ensure that an appropriate `Expiration date` is set.

Audit from Azure CLI

Get a list of all the key vaults in your Azure environment by running the following command:

```
az keyvault list
```

For each key vault, ensure that the output of the below command contains Key ID (kid), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault key list --vault-name <KEYVAULTNAME> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Azure Key vaults:

```
Get-AzKeyVault
```

For each Key vault, run the following command to determine which vaults are configured to not use RBAC:

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key vault with the `EnableRbacAuthorizatoin` setting set to `False` or empty, run the following command.

```
Get-AzKeyVaultKey -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

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:** 152b15f7-8e1f-4c1f-ab71-8c010ba5dbc0 **- Name:** 'Key Vault keys should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that the status of the key is `Enabled`.
4. For each enabled key, ensure that an appropriate `Expiration date` is set.

Remediate from Azure CLI
Update the `Expiration date` for the key using the below command:

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --
expires Y-m-d'T'H:M:S'Z'
```

Note:
To view the expiration date on all keys in a Key Vault using Microsoft API, the "List" Key permission is required.
To update the expiration date for the keys:

1. Go to Key vault, click on `Access policies`.
2. Click on `Create` and add an access policy with the `Update` permission (in the Key Permissions - Key Management Operations section).

Remediate from PowerShell

```
Set-AzKeyVaultKeyAttribute -VaultName <Vault Name> -Name <Key Name> -Expires
<DateTime>
```

Default Value:

By default, keys do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-keys
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyattribute?view=azps-0.10.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1047

9.3.3 Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Secrets in Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The `exp` (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Impact:

Secrets cannot be used beyond their assigned expiry date respectively. Secrets need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Secrets`.
3. In the main pane, ensure that the status of the secret is `Enabled`.
4. For each enabled secret, ensure that an appropriate `Expiration date` is set.

Audit from Azure CLI

Ensure that the output of the below command contains ID (id), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault secret list --vault-name <KEYVAULTNAME> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Key vaults:

```
Get-AzKeyVault
```

For each Key vault, run the following command to determine which vaults are configured to use RBAC:

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key vault with the EnableRbacAuthorization setting set to True, run the following command:

```
Get-AzKeyVaultSecret -VaultName <Vault Name>
```

Make sure the Expires setting is configured with a value as appropriate wherever the Enabled setting is set to True.

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:** 98728c90-32c7-4049-8429-847dc0f4fe37 **- Name:** 'Key Vault secrets should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to Key vaults.
2. For each Key vault, click on Secrets.
3. In the main pane, ensure that the status of the secret is Enabled.
4. For each enabled secret, ensure that an appropriate Expiration date is set.

Remediate from Azure CLI
Update the Expiration date for the secret using the below command:

```
az keyvault secret set-attributes --name <secret_name> --vault-name
<vault_name> --expires Y-m-d'T'H:M:S'Z'
```

Note:
To view the expiration date on all secrets in a Key Vault using Microsoft API, the List Secret permission is required.
To update the expiration date for the secrets:

1. Go to the Key vault, click on Access Control (IAM).
2. Click on Add role assignment and assign the role of Key Vault Secrets Officer to the appropriate user.

Remediate from PowerShell

```
Set-AzKeyVaultSecretAttribute -VaultName <vault_name> -Name <secret_name> -
Expires <date_time>
```

Default Value:

By default, secrets do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-secrets
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultsecretattribute?view=azps-0.10.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1047

9.3.4 Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Secrets in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The `exp` (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Impact:

Secrets cannot be used beyond their assigned expiry date respectively. Secrets need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Secrets`.
3. In the main pane, ensure that the status of the secret is `Enabled`.
4. Set an appropriate `Expiration date` on all secrets.

Audit from Azure CLI

Get a list of all the key vaults in your Azure environment by running the following command:

```
az keyvault list
```

For each key vault, ensure that the output of the below command contains ID (id), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault secret list --vault-name <KEYVALUTNAME> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Key vaults:

```
Get-AzKeyVault
```

For each Key vault run the following command to determine which vaults are configured to use RBAC:

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key Vault with the `EnableRbacAuthorization` setting set to `False` or empty, run the following command.

```
Get-AzKeyVaultSecret -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

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:** 98728c90-32c7-4049-8429-847dc0f4fe37 **- Name:** 'Key Vault secrets should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Secrets`.
3. In the main pane, ensure that the status of the secret is `Enabled`.
4. Set an appropriate `Expiration date` on all secrets.

Remediate from Azure CLI
Update the `Expiration date` for the secret using the below command:

```
az keyvault secret set-attributes --name <secret_name> --vault-name
<vault_name> --expires Y-m-d'T'H:M:S'Z'
```

Note: To view the expiration date on all secrets in a Key Vault using Microsoft API, the `List` Secret permission is required.
To update the expiration date for the secrets:

1. Go to Key vault, click on `Access policies`.
2. Click on `Create` and add an access policy with the `Update` permission (in the Secret Permissions - Secret Management Operations section).

Remediate from PowerShell
For each Key vault with the `EnableRbacAuthorization` setting set to `False` or empty, run the following command.

```
Set-AzKeyVaultSecret -VaultName <vault_name> -Name <secret_name> -Expires
<date_time>
```

Default Value:

By default, secrets do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-secrets
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultsecret?view=azps-7.4.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1047

9.3.5 Ensure the Key Vault is Recoverable (Automated)

Profile Applicability:

- Level 1

Description:

Key Vaults contain object keys, secrets, and certificates. Deletion of a Key Vault can cause immediate data loss or loss of security functions (authentication, validation, verification, non-repudiation, etc.) supported by the Key Vault objects.

It is recommended the Key Vault be made recoverable by enabling the "Do Not Purge" and "Soft Delete" functions. This is in order to prevent loss of encrypted data, including storage accounts, SQL databases, and/or dependent services provided by Key Vault objects (Keys, Secrets, Certificates) etc. This may happen in the case of accidental deletion by a user or from disruptive activity by a malicious user.

NOTE: In February 2025, Microsoft will enable soft-delete protection on all key vaults, and users will no longer be able to opt out of or turn off soft-delete.

WARNING: A current limitation is that role assignments disappearing when Key Vault is deleted. All role assignments will need to be recreated after recovery.

Rationale:

Users may accidentally run delete/purge commands on a Key Vault, or an attacker or malicious user may do so deliberately in order to cause disruption. Deleting or purging a Key Vault leads to immediate data loss, as keys encrypting data and secrets/certificates allowing access/services will become non-accessible.

Setting `enablePurgeProtection` to "true" for a Key Vault ensures that even if Key Vault is deleted, Key Vault itself or its objects remain recoverable for the next 90 days. Key Vault/objects can either be recovered or purged (permanent deletion) during those 90 days. If no action is taken, the key vault and its objects will subsequently be purged.

Enabling the enablePurgeProtection parameter on Key Vaults ensures that Key Vaults and their objects cannot be deleted/purged permanently.

Impact:

Once purge-protection and soft-delete are enabled for a Key Vault, the action is irreversible.

Audit:

Audit from Azure Portal

1. Go to `Key Vaults`.
2. Click the name of a Key Vault.
3. Under `Settings`, click `Properties`.

4. Next to `Purge protection`, ensure that `Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)` is selected.
5. Repeat steps 1-4 for each Key Vault.

Audit from Azure CLI
List all Key Vaults:

```
az resource list --query "[?type=='Microsoft.KeyVault/vaults']"
```

For each Key Vault, ensure `enablePurgeProtection` is set to true:

```
az resource show --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName>
```

Audit from PowerShell
List all Key Vaults:

```
Get-AzKeyVault
```

For each Key Vault run the following command:

```
Get-AzKeyVault -VaultName <Vault Name>
```

Ensure `EnablePurgeProtection` is set to `True`.

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:** 0b60c0b2-2dc2-4e1c-b5c9-abbed971de53 **- Name:** 'Key vaults should have deletion protection enabled'

Remediation:

To enable "Do Not Purge" and "Soft Delete" for a Key Vault:
Remediate from Azure Portal

1. Go to `Key Vaults`.
2. Click the name of a Key Vault.
3. Under `Settings`, click `Properties`.
4. Select the radio button next to `Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)`.
   Note: Once enabled, this option cannot be disabled.
5. Click `Save`.
6. Repeat steps 1-5 for each Key Vault requiring remediation.

Remediate from Azure CLI

```
az resource update --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName> --set properties.enablePurgeProtection=true
```

Remediate from PowerShell

```
Update-AzKeyVault -VaultName <vaultName -ResourceGroupName <resourceGroupName
-EnablePurgeProtection
```

Default Value:

When a new Key Vault is created,

- `enableSoftDelete` is enabled by default, and
- `enablePurgeProtection` is disabled by default.

NOTE: In February 2025, Microsoft will enable soft-delete protection on all key vaults, and users will no longer be able to opt out of or turn off soft-delete.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-soft-delete-cli
2. https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-8-define-and-implement-backup-and-recovery-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository

Additional Information:

When a key is used for SQL server TDE or Encrypting Storage Account, both the features "Do Not Purge" and "Soft Delete" are enabled for the corresponding Key Vault by default by Azure Backend.

WARNING: A current limitation of the soft-delete feature across all Azure services is role assignments disappearing when Key Vault is deleted. All role assignments will need to be recreated after recovery.

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	10.2 Perform Complete System Backups Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

9.3.6 Ensure that Role Based Access Control for Azure Key Vault is enabled (Automated)

Profile Applicability:

- Level 2

Description:

The recommended way to access Key Vaults is to use the Azure Role-Based Access Control (RBAC) permissions model.

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources. It allows users to manage Key, Secret, and Certificate permissions. It provides one place to manage all permissions across all key vaults.

Rationale:

The new RBAC permissions model for Key Vaults enables a much finer grained access control for key vault secrets, keys, certificates, etc., than the vault access policy. This in turn will permit the use of privileged identity management over these roles, thus securing the key vaults with JIT Access management.

Impact:

Implementation needs to be properly designed from the ground up, as this is a fundamental change to the way key vaults are accessed/managed. Changing permissions to key vaults will result in loss of service as permissions are re-applied. For the least amount of downtime, map your current groups and users to their corresponding permission needs.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left corner
2. Select Key Vaults
3. Select a Key Vault to audit
4. Select Access configuration
5. Ensure the Permission Model radio button is set to `Azure role-based access control`

Audit from Azure CLI

Run the following command for each Key Vault in each Resource Group:

```
az keyvault show --resource-group <resource_group> --name <vault_name>
```

Ensure the `enableRbacAuthorization` setting is set to `true` within the output of the above command.

Audit from PowerShell
Run the following PowerShell command:

```
Get-AzKeyVault -Vaultname <vault_name> -ResourceGroupName <resource_group>
```

Ensure the `Enabled For RBAC Authorization` setting is set to `True`
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:** 12d4fa5e-1f9f-4c21-97a9-b99b3c6611b5 **- Name:** 'Azure Key Vault should use RBAC permission model'

Remediation:

Remediate from Azure Portal
Key Vaults can be configured to use `Azure role-based access control` on creation. For existing Key Vaults:

1. From Azure Home open the Portal Menu in the top left corner
2. Select `Key Vaults`
3. Select a Key Vault to audit
4. Select `Access configuration`
5. Set the Permission model radio button to `Azure role-based access control`, taking note of the warning message
6. Click `Save`
7. Select `Access Control (IAM)`
8. Select the `Role Assignments` tab
9. Reapply permissions as needed to groups or users

Remediate from Azure CLI
To enable RBAC Authorization for each Key Vault, run the following Azure CLI command:

```
az keyvault update --resource-group <resource_group> --name <vault_name> --
enable-rbac-authorization true
```

Remediate from PowerShell
To enable RBAC authorization on each Key Vault, run the following PowerShell command:

```
Update-AzKeyVault -ResourceGroupName <resource_group> -VaultName <vault_name>
-EnableRbacAuthorization $True
```

Default Value:

The default value for Access control in Key Vaults is Vault Policy.

References:

1. https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-migration#vault-access-policy-to-azure-rbac-migration-steps
2. https://docs.microsoft.com/en-gb/azure/role-based-access-control/role-assignments-portal?tabs=current
3. https://docs.microsoft.com/en-gb/azure/role-based-access-control/overview
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository

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.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1047

9.3.7 Ensure that Public Network Access when using Private Endpoint is disabled (Automated)

Profile Applicability:

- Level 2

Description:

When Private endpoint is configured on a Key Vault, connections from Azure resources within the same subnet will use its private IP address. However, network traffic from the public internet can still flow connect to the Key Vault's public endpoint (mykeyvault.vault.azure.net) using its public IP address unless Public network access is set to "Disabled".

Setting the Public network access to "Disabled" with a Private Endpoint will remove the Vault's public endpoint from Azure public DNS, reducing its exposure to the public internet. Network traffic will use the Vault private endpoint IP address for all requests (mykeyvault.vault.privatelink.azure.net).

Rationale:

Removing a point of interconnection from the internet edge to your Key Vault can strengthen the network security boundary of your system and reduce the risk of exposing the control plane or vault objects to untrusted clients.

Although Azure resources are never truly isolated from the public internet, disabling the public endpoint removes a line of sight from the public internet and increases the effort required for an attack.

Impact:

Implementation needs to be properly designed from the ground up, as this is a fundamental change to the network architecture of your system. It will increase the configuration effort and decrease the usability of the Key Vault, and is appropriate for workloads where security is the primary consideration.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left corner
2. Select Key Vaults
3. Select a Key Vault to audit
4. Select Networking
5. Ensure that Public network access is Disabled.
6. Ensure that a Private endpoint is provisioned and connected.

Audit from Azure CLI
Run the following command for each Key Vault in each Resource Group:

```
az keyvault show --resource-group <resource_group> --name <vault_name>
```

Ensure the `publicNetworkSetting` setting is set to `Disabled` within the output of the above command.

Audit from PowerShell
Run the following PowerShell command:

```
Get-AzKeyVault -Vaultname <vault_name> -ResourceGroupName <resource_group>
```

Ensure the `Public network access` setting is set to `Disabled`

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:** 405c5871-3e91-4644-8a63-58e19d68ff5b **- Name:** 'Azure Key Vault should disable public network access'

Remediation:

Remediate from Azure Portal
Key Vaults can be configured to use `Azure role-based access control` on creation. For existing Key Vaults:

1. From Azure Home open the Portal Menu in the top left corner
2. Select `Key Vaults`
3. Select a Key Vault to audit
4. Select `Networking`
5. NEXT

Remediate from Azure CLI
To disable Public network access for each Key Vault, run the following Azure CLI command:

```
az keyvault update --resource-group <resource_group> --name <vault_name> --
public-network-access Disabled
```

Remediate from PowerShell
To enable RBAC authorization on each Key Vault, run the following PowerShell command:

```
Update-AzKeyVault -ResourceGroupName <resource_group> -VaultName <vault_name>
-PublicNetworkAccess "Disabled"
```

Default Value:

The default value for Access control in Key Vaults is Vault Policy.

References:

1. https://learn.microsoft.com/en-us/azure/key-vault/general/network-security
2. https://learn.microsoft.com/en-us/azure/key-vault/general/private-link-service

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.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1047

9.3.8 Ensure that Private Endpoints are Used for Azure Key Vault (Automated)

Profile Applicability:

- Level 2

Description:

Private endpoints will secure network traffic from Azure Key Vault to the resources requesting secrets and keys.

Rationale:

Private endpoints will keep network requests to Azure Key Vault limited to the endpoints attached to the resources that are whitelisted to communicate with each other. Assigning the Key Vault to a network without an endpoint will allow other resources on that network to view all traffic from the Key Vault to its destination. In spite of the complexity in configuration, this is recommended for high security secrets.

Impact:

Incorrect or poorly-timed changing of network configuration could result in service interruption. There are also additional costs tiers for running a private endpoint per petabyte or more of networking traffic.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Select `Networking` in the left column.
5. Select `Private endpoint connections` from the top row.
6. View if there is an endpoint attached.

Audit from Azure CLI

Run the following command within a subscription for each Key Vault you wish to audit.

```
az keyvault show --name <keyVaultName>
```

Ensure that `privateEndpointConnections` is not `null`.

Audit from PowerShell

Run the following command within a subscription for each Key Vault you wish to audit.

```
Get-AzPrivateEndpointConnection -PrivateLinkResourceId
'/subscriptions/<subscriptionNumber>/resourceGroups/<resourceGroup>/providers
/Microsoft.KeyVault/vaults/<keyVaultName>/'
```

Ensure that the response contains details of a private endpoint.

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:** a6abeaec-4d90-4a02-805f-6b26c4d3fbe9 **- Name:** 'Azure Key Vaults should use private link'

Remediation:

Please see the additional information about the requirements needed before starting this remediation procedure.
Remediate from Azure Portal

1. From Azure Home open the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Select `Networking` in the left column.
5. Select `Private endpoint connections` from the top row.
6. Select `+ Create`.
7. Select the subscription the Key Vault is within, and other desired configuration.
8. Select `Next`.
9. For resource type select `Microsoft.KeyVault/vaults`.
10. Select the Key Vault to associate the Private Endpoint with.
11. Select `Next`.
12. In the `Virtual Networking` field, select the network to assign the Endpoint.
13. Select other configuration options as desired, including an existing or new application security group.
14. Select `Next`.
15. Select the private DNS the Private Endpoints will use.
16. Select `Next`.
17. Optionally add `Tags`.
18. Select `Next : Review + Create`.
19. Review the information and select `Create`. Follow the Audit Procedure to determine if it has successfully applied.
20. Repeat steps 3-19 for each Key Vault.

Remediate from Azure CLI

1. To create an endpoint, run the following command:

```
az network private-endpoint create --resource-group <resourceGroup --vnet-
name <vnetName> --subnet <subnetName> --name <PrivateEndpointName>  --
private-connection-resource-id "/subscriptions/<AZURE SUBSCRIPTION
ID>/resourceGroups/<resourceGroup>/providers/Microsoft.KeyVault/vaults/<keyVa
ultName>" --group-ids vault --connection-name <privateLinkConnectionName> --
location <azureRegion> --manual-request
```

2. To manually approve the endpoint request, run the following command:

```
az keyvault private-endpoint-connection approve --resource-group
<resourceGroup> --vault-name <keyVaultName> –name <privateLinkName>
```

3. Determine the Private Endpoint's IP address to connect the Key Vault to the Private DNS you have previously created:
4. Look for the property networkInterfaces then id; the value must be placed in the variable <privateEndpointNIC> within step 7.

```
az network private-endpoint show -g <resourceGroupName> -n
<privateEndpointName>
```

5. Look for the property networkInterfaces then id; the value must be placed on <privateEndpointNIC> in step 7.

```
az network nic show --ids <privateEndpointName>
```

6. Create a Private DNS record within the DNS Zone you created for the Private Endpoint:

```
az network private-dns record-set a add-record -g <resourcecGroupName> -z
"privatelink.vaultcore.azure.net" -n <keyVaultName> -a <privateEndpointNIC>
```

7. nslookup the private endpoint to determine if the DNS record is correct:

```
nslookup <keyVaultName>.vault.azure.net
nslookup <keyVaultName>.privatelink.vaultcore.azure.n
```

Default Value:

By default, Private Endpoints are not enabled for any services within Azure.

References:

1. https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview

2. https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints
3. https://azure.microsoft.com/en-us/pricing/details/private-link/
4. https://docs.microsoft.com/en-us/azure/key-vault/general/private-link-service?tabs=portal
5. https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-portal
6. https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal
7. https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
8. https://docs.microsoft.com/azure/dns/private-dns-getstarted-cli#create-an-additional-dns-record
9. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository

Additional Information:

This recommendation assumes that you have created a Resource Group containing a Virtual Network that the services are already associated with and configured private DNS. A Bastion on the virtual network is also required, and the service to which you are connecting must already have a Private Endpoint. For information concerning the installation of these services, please see the attached documentation.

Microsoft's own documentation lists the requirements as: A Key Vault. An Azure virtual network. A subnet in the virtual network. Owner or contributor permissions for both the Key Vault and the virtual network.

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	14.1 Segment the Network Based on Sensitivity 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).		●	●

9.3.9 Ensure automatic key rotation is enabled within Azure Key Vault (Automated)

Profile Applicability:

- Level 2

Description:

Automated cryptographic key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. A key rotation policy can be defined for each individual key.

Rationale:

Automatic key rotation reduces risk by ensuring that keys are rotated without manual intervention.

Azure and NIST recommend that keys be rotated every two years or less. Refer to 'Table 1: Suggested cryptoperiods for key types' on page 46 of the following document for more information: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

Impact:

There is an additional cost for each scheduled key rotation.

Audit:

Audit from Azure Portal

1. Go to `Key Vaults`.
2. Select a Key Vault.
3. Under `Objects`, select `Keys`.
4. Select a key.
5. From the top row, select `Rotation policy`.
6. Ensure `Enable auto rotation` is set to `Enabled`.
7. Ensure the `Rotation time` is set to an appropriate value.
8. Repeat steps 1-7 for each Key Vault and Key.

Audit from Azure CLI
Run the following command:

```
az keyvault key rotation-policy show --vault-name <vault-name> --name <key-name>
```

Ensure that the response contains a `lifetimeAction` of `Rotate` and that `timeAfterCreate` is set to an appropriate value.

Audit from PowerShell
Run the following command:

```
Get-AzKeyVaultKeyRotationPolicy -VaultName <vault-name> -Name <key-name>
```

Ensure that the response contains a `LifetimeAction` of `Rotate` and that `TimeAfterCreate` is set to an appropriate value.

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:** d8cf8476-a2ec-4916-896e-992351803c44 **- Name:** 'Keys should have a rotation policy ensuring that their rotation is scheduled within the specified number of days after creation.'

Remediation:

Note: Azure CLI and PowerShell use the ISO8601 duration format for time spans. The format is `P<timespanInISO8601Format>(Y,M,D)`. The leading P is required and is referred to as `period`. The `(Y,M,D)` are for the duration of Year, Month, and Day, respectively. A time frame of 2 years, 2 months, 2 days would be `P2Y2M2D`. For Azure CLI and PowerShell, it is easiest to supply the policy flags in a `.json file`, for example:

```
{
  "lifetimeActions": [
    {
      "trigger": {
        "timeAfterCreate": "P<timespanInISO8601Format>(Y,M,D)",
        "timeBeforeExpiry" : null
      },
      "action": {
        "type": "Rotate"
      }
    },
    {
      "trigger": {
        "timeBeforeExpiry" : "P<timespanInISO8601Format>(Y,M,D)"
      },
      "action": {
        "type": "Notify"
      }
    }
  ],
  "attributes": {
    "expiryTime": "P<timespanInISO8601Format>(Y,M,D)"
  }
}
```

Remediate from Azure Portal

1. Go to `Key Vaults`.
2. Select a Key Vault.
3. Under `Objects`, select `Keys`.
4. Select a key.
5. From the top row, select `Rotation policy`.
6. Select an appropriate `Expiry time`.
7. Set `Enable auto rotation` to `Enabled`.
8. Set an appropriate `Rotation option` and `Rotation time`.
9. Optionally, set a `Notification time`.
10. Click `Save`.
11. Repeat steps 1-10 for each Key Vault and Key.

Remediate from Azure CLI

Run the following command for each key to enable automatic rotation:

```
az keyvault key rotation-policy update --vault-name <vault-name> --name <key-name> --value <path/to/policy.json>
```

Remediate from PowerShell

Run the following command for each key to enable automatic rotation:

```
Set-AzKeyVaultKeyRotationPolicy -VaultName <vault-name> -Name <key-name> -PolicyPath <path/to/policy.json>
```

Default Value:

By default, automatic key rotation is not enabled.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation
2. https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#update-the-key-version
3. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell#set-up-an-azure-key-vault-and-diskencryptionset-optionally-with-automatic-key-rotation
4. https://azure.microsoft.com/en-us/updates/public-preview-automatic-key-rotation-of-customermanaged-keys-for-encrypting-azure-managed-disks/
5. https://docs.microsoft.com/en-us/cli/azure/keyvault/key/rotation-policy?view=azure-cli-latest#az-keyvault-key-rotation-policy-update
6. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyrotationpolicy?view=azps-8.1.0
7. https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/scalar-data-types/timespan
8. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
9. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1041

9.3.10 Ensure that Azure Key Vault Managed HSM is used when required (Manual)

Profile Applicability:

- Level 2

Description:

Azure Key Vault Managed HSM is a fully managed, highly available, single-tenant cloud service that safeguards cryptographic keys using FIPS 140-2 Level 3 validated HSMs.

Note: This recommendation to use Managed HSM applies only to scenarios where specific regulatory and compliance requirements mandate the use of a dedicated hardware security module.

Rationale:

Managed HSM is a fully managed, highly available, single-tenant service that ensures FIPS 140-2 Level 3 compliance. It provides centralized key management, isolated access control, and private endpoints for secure access. Integrated with Azure services, it supports migration from Key Vault, ensures data residency, and offers monitoring and auditing for enhanced security.

Impact:

Managed HSM incurs a cost of $0.40 to $5 per month for each actively used HSM-protected key, depending on the key type and quantity. Each key version is billed separately. Additionally, there is an hourly usage fee of $3.20 per Managed HSM pool.

Audit:

Audit from Azure CLI
Run the following command to list key vaults:

```
az keyvault list --query [*].[name,type]
```

Ensure that at least one key vault with type `Microsoft.KeyVault/managedHSMs` exists.

Remediation:

Remediate from Azure CLI
Run the following command to set `oid` to be the `OID` of the signed-in user:

```
$oid = az ad signed-in-user show --query id -o tsv
```

Alternatively, prepare a space-separated list of OIDs to be provided as the `administrators` of the HSM.
Run the following command to create a Managed HSM:

```
az keyvault create --resource-group <resource-group> --hsm-name <hsm-name> --
retention-days <retention-days> --administrators $oid
```

The command can take several minutes to complete.
After the HSM has been created, it must be activated before it can be used. Activation requires providing a minimum of three and a maximum of ten RSA key pairs, as well as the minimum number of keys required to decrypt the security domain (called a quorum).
OpenSSL can be used to generate the self-signed certificates, for example:

```
openssl req -newkey rsa:2048 -nodes -keyout cert_1.key -x509 -days 365 -out
cert_1.cer
```

Run the following command to download the security domain and activate the Managed HSM:

```
az keyvault security-domain download --hsm-name <managed-hsm> --sd-wrapping-
keys <key-1> <key-2> <key-3> --sd-quorum <quorum> --security-domain-file
<managed-hsm-security-domain>.json
```

Store the security domain file and the RSA key pairs securely. They will be required for disaster recovery or for creating another Managed HSM that shares the same security domain so that the two can share keys.
The Managed HSM will now be in an active state and ready for use.

References:

1. https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management-choose
2. https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview
3. https://azure.microsoft.com/en-gb/pricing/details/key-vault/
4. https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/quick-create-cli
5. https://learn.microsoft.com/en-us/cli/azure/keyvault

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 Segment Data Processing and Storage Based on Sensitivity Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		●	●
v7	2.10 Physically or Logically Segregate High Risk Applications Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1552	TA0006	M1041

9.4 Azure Bastion

9.4.1 Ensure an Azure Bastion Host Exists (Automated)

Profile Applicability:

- Level 2

Description:

The Azure Bastion service allows secure remote access to Azure Virtual Machines over the Internet without exposing remote access protocol ports and services directly to the Internet. The Azure Bastion service provides this access using TLS over 443/TCP, and subscribes to hardened configurations within an organization's Azure Active Directory service.

Rationale:

The Azure Bastion service allows organizations a more secure means of accessing Azure Virtual Machines over the Internet without assigning public IP addresses to those Virtual Machines. The Azure Bastion service provides Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Virtual Machines using TLS within a web browser, thus preventing organizations from opening up 3389/TCP and 22/TCP to the Internet on Azure Virtual Machines. Additional benefits of the Bastion service includes Multi-Factor Authentication, Conditional Access Policies, and any other hardening measures configured within Azure Active Directory using a central point of access.

Impact:

The Azure Bastion service incurs additional costs and requires a specific virtual network configuration. The `Standard` tier offers additional configuration options compared to the `Basic` tier and may incur additional costs for those added features.

Audit:

Audit from Azure Portal

1. Click on `Bastions`
2. Ensure there is at least one `Bastion` host listed under the `Name` column

Audit from Azure CLI
Note: The Azure CLI `network bastion` module is in `Preview` as of this writing

```
az network bastion list --subscription <subscription ID>
```

Ensure the output of the above command is not empty.

Audit from PowerShell
Retrieve the `Bastion` host(s) information for a specific `Resource Group`

```
Get-AzBastion -ResourceGroupName <resource group name>
```

Ensure the output of the above command is not empty.

Remediation:

Remediate from Azure Portal

1. Click on Bastions
2. Select the Subscription
3. Select the Resource group
4. Type a Name for the new Bastion host
5. Select a Region
6. Choose Standard next to Tier
7. Use the slider to set the Instance count
8. Select the Virtual network or Create new
9. Select the Subnet named AzureBastionSubnet. Create a Subnet named AzureBastionSubnet using a /26 CIDR range if it doesn't already exist.
10. Select the appropriate Public IP address option.
11. If Create new is selected for the Public IP address option, provide a Public IP address name.
12. If Use existing is selected for Public IP address option, select an IP address from Choose public IP address
13. Click Next: Tags >
14. Configure the appropriate Tags
15. Click Next: Advanced >
16. Select the appropriate Advanced options
17. Click Next: Review + create >
18. Click Create

Remediate from Azure CLI

```
az network bastion create --location <location> --name <name of bastion host>
--public-ip-address <public IP address name or ID> --resource-group <resource
group name or ID> --vnet-name <virtual network containing subnet called
"AzureBastionSubnet"> --scale-units <integer> --sku Standard [--disable-copy-
paste true|false] [--enable-ip-connect true|false] [--enable-tunneling
true|false]
```

Remediate from PowerShell

Create the appropriate Virtual network settings and Public IP Address settings.

```
$subnetName = "AzureBastionSubnet"
$subnet = New-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix
<IP address range in CIDR notation making sure to use a /26>
$virtualNet = New-AzVirtualNetwork -Name <virtual network name> -
ResourceGroupName <resource group name> -Location <location> -AddressPrefix
<IP address range in CIDR notation> -Subnet $subnet
$publicip = New-AzPublicIpAddress -ResourceGroupName <resource group name> -
Name <public IP address name> -Location <location> -AllocationMethod Dynamic
-Sku Standard
```

Create the Azure Bastion service using the information within the created variables from above. *[next page]*

```
New-AzBastion -ResourceGroupName <resource group name> -Name <bastion name> -
PublicIpAddress $publicip -VirtualNetwork $virtualNet -Sku "Standard" -
ScaleUnit <integer>
```

Default Value:

By default, the Azure Bastion service is not configured.

References:

1. https://learn.microsoft.com/en-us/azure/bastion/bastion-overview#sku
2. https://learn.microsoft.com/en-us/powershell/module/az.network/get-azbastion?view=azps-9.2.0
3. https://learn.microsoft.com/en-us/cli/azure/network/bastion?view=azure-cli-latest

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.1 Ensure Network Infrastructure is Up-to-Date Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1557	TA0006	M1035

10 Storage Services

SERVICE CATEGORY BENCHMARK AVAILABLE

- "CIS Microsoft Azure Storage Services Benchmark"

To better understand the relationship between the Foundations Benchmark and Services Benchmarks, please read the "Introduction" section of this document.

PARTIAL RELOCATION - BE ADVISED!

Some recommendations previously covered in the CIS Microsoft Azure Foundations Benchmark (this document) related to Storage services have been relocated to a Benchmark titled **CIS Microsoft Azure Storage Services Benchmark**. This Storage Services section now provides a **foundational set** of secure configuration recommendations for products from Azure Product Directory's "Storage" category of services.

After applying foundational recommendations, take inventory of the entire set of Storage Services in use by your organization, then look to the Benchmarks section of the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72) for defense-in-depth guidance for those specific services in the **CIS Microsoft Azure Storage Services Benchmark**.

Services addressed in the **CIS Microsoft Azure Storage Services Benchmark**:

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

Azure Product Directory Reference: https://azure.microsoft.com/en-us/products#storage

FEEDBACK REQUEST: Is there a specific service or recommendation in this section that you'd like to see addressed or improved? Let us know by making a ticket or starting a discussion in the CIS Microsoft Azure Community (https://workbench.cisecurity.org/communities/72).

10.1 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

10.1.1 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 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

10.1.2 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 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1042

10.1.3 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 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1210	TA0008	M1042

10.2 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.

NOTE: If your organization is using Shared Access Signature (SAS) tokens, please review the CIS Microsoft Azure Storage Services Benchmark for best practice guidance on the configuration and use of those tokens.

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

10.2.1 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 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

10.2.2 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.

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:** c36a325b-ae04-4863-ad4f-19c6678f8e08 **- Name:** 'Configure your Storage account to enable blob versioning'

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

10.3 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

10.3.1 Secrets and Keys

10.3.1.1 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.

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 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 are 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-privilegedadministrative-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 Establish and Maintain a Secure Configuration Process 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 Use Automated Tools to Verify Standard Device Configurations and Detect Changes Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

10.3.1.2 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 or 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 the 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-privilegedadministrative-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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1098	TA0003	M1026

10.3.1.3 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 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.	●	●	●
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	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.	●	●	●
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.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1022

10.3.2 Networking

10.3.2.1 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:

If an Azure Virtual Network is not implemented correctly, this may result in the loss of critical network traffic.

Private endpoints are charged per hour of use. Refer to https://azure.microsoft.com/en-us/pricing/details/private-link/ and https://azure.microsoft.com/en-us/pricing/calculator/ to estimate potential costs.

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.

This recommendation is based on the Common Reference Recommendation `Ensure Private Endpoints are used to access {service}`, from the `Common Reference Recommendations > Networking > Private Endpoints` section.

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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.1 Segment the Network Based on Sensitivity 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).		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1537	TA0010	M1037

10.3.2.2 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-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
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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1037

10.3.2.3 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 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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1037

10.3.3 Identity and Access Management

10.3.3.1 Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1

Description:

When this property is enabled, the Azure portal authorizes requests to blobs, files, queues, and tables with Microsoft Entra ID by default.

Rationale:

Microsoft Entra ID provides superior security and ease of use over Shared Key.

Audit:

Audit from Azure Portal

1. Go to `Storage accounts`.
2. Click the name of a storage account.
3. Under `Settings`, click `Configuration`.
4. Ensure that `Default to Microsoft Entra authorization in the Azure portal` is set to `Enabled`.
5. Repeat steps 1-4 for each storage account.

Audit from Azure CLI
Run the following command to get the `name` and `defaultToOAuthAuthentication` setting for each storage account:

```
az storage account list --query [*].[name,defaultToOAuthAuthentication]
```

Ensure that `true` is returned for each storage account.

Remediation:

Remediate from Azure Portal

1. Go to `Storage accounts`.
2. Click the name of a storage account.
3. Under `Settings`, click `Configuration`.
4. Under `Default to Microsoft Entra authorization in the Azure portal`, click the radio button next to `Enabled`.
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 `defaultToOAuthAuthentication`:

```
az storage account update --resource-group <resource-group> --name <storage-account> --set defaultToOAuthAuthentication=true
```

Default Value:

By default, `defaultToOAuthAuthentication` is disabled.

References:

1. https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal#default-to-microsoft-entra-authorization-in-the-azure-portal
2. https://learn.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest

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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1022

10.3.4 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 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

10.3.5 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 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.	●	●	●
v8	13.5 Manage Access Control for Remote Assets 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 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.			●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1530	TA0009	M1037

10.3.6 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 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

10.3.7 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 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

10.3.8 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 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	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.		●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1565.001	TA1020	M1022

10.3.9 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:** '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 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.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1567	TA0010	M1057

10.3.10 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 Data Protection Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485, T1490	TA0040	

10.3.11 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.			

10.3.12 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 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 Data Recovery Capabilities Data Recovery Capabilities			

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1485	TA0040	M1053

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3	**Analytics Services**		
3.1	**Azure Databricks**		
3.1.1	Ensure that Azure Databricks is deployed in a customer-managed virtual network (VNet) (Automated)	☐	☐
3.1.2	Ensure that network security groups are configured for Databricks subnets (Manual)	☐	☐
3.1.3	Ensure that traffic is encrypted between cluster worker nodes (Manual)	☐	☐
3.1.4	Ensure that users and groups are synced from Microsoft Entra ID to Azure Databricks (Manual)	☐	☐
3.1.5	Ensure that Unity Catalog is configured for Azure Databricks (Manual)	☐	☐
3.1.6	Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens (Manual)	☐	☐
3.1.7	Ensure that diagnostic log delivery is configured for Azure Databricks (Manual)	☐	☐
3.1.8	Ensure that data at rest and in transit is encrypted in Azure Databricks using customer managed keys (CMK) (Automated)	☐	☐
4	**Compute Services**		
4.1	**Virtual Machines**		
4.1.1	Ensure only MFA enabled identities can access privileged Virtual Machine (Manual)	☐	☐
5	**Database Services (reference)**		
6	**Identity Services**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1	**Security Defaults (Per-User MFA)**		
6.1.1	Ensure that 'security defaults' is enabled in Microsoft Entra ID (Manual)	☐	☐
6.1.2	Ensure that 'multifactor authentication' is 'enabled' for all users (Manual)	☐	☐
6.1.3	Ensure that 'Allow users to remember multifactor authentication on devices they trust' is disabled (Manual)	☐	☐
6.2	**Conditional Access**		
6.2.1	Ensure that 'trusted locations' are defined (Manual)	☐	☐
6.2.2	Ensure that an exclusionary geographic Conditional Access policy is considered (Manual)	☐	☐
6.2.3	Ensure that an exclusionary device code flow policy is considered (Manual)	☐	☐
6.2.4	Ensure that a multifactor authentication policy exists for all users (Manual)	☐	☐
6.2.5	Ensure that multifactor authentication is required for risky sign-ins (Manual)	☐	☐
6.2.6	Ensure that multifactor authentication is required for Windows Azure Service Management API (Manual)	☐	☐
6.2.7	Ensure that multifactor authentication is required to access Microsoft Admin Portals (Manual)	☐	☐
6.3	**Periodic Identity Reviews**		
6.3.1	Ensure that Azure admin accounts are not used for daily operations (Manual)	☐	☐
6.3.2	Ensure that guest users are reviewed on a regular basis (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.3.3	Ensure that use of the 'User Access Administrator' role is restricted (Automated)	☐	☐
6.3.4	Ensure that all 'privileged' role assignments are periodically reviewed (Manual)	☐	☐
6.4	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated)	☐	☐
6.5	Ensure that 'Number of methods required to reset' is set to '2' (Manual)	☐	☐
6.6	Ensure that account 'Lockout threshold' is less than or equal to '10' (Manual)	☐	☐
6.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60' (Manual)	☐	☐
6.8	Ensure that a 'Custom banned password list' is set to 'Enforce' (Manual)	☐	☐
6.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual)	☐	☐
6.10	Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)	☐	☐
6.11	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)	☐	☐
6.12	Ensure that 'User consent for applications' is set to 'Do not allow user consent' (Manual)	☐	☐
6.13	Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions' (Manual)	☐	☐
6.14	Ensure that 'Users can register applications' is set to 'No' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.15	Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Automated)	☐	☐
6.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' (Automated)	☐	☐
6.17	Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes' (Manual)	☐	☐
6.18	Ensure that 'Restrict user ability to access groups features in My Groups' is set to 'Yes' (Manual)	☐	☐
6.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual)	☐	☐
6.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No' (Manual)	☐	☐
6.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual)	☐	☐
6.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes' (Manual)	☐	☐
6.23	Ensure that no custom subscription administrator roles exist (Automated)	☐	☐
6.24	Ensure that a custom role is assigned permissions for administering resource locks (Manual)	☐	☐
6.25	Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one' (Manual)	☐	☐
6.26	Ensure fewer than 5 users have global administrator assignment (Manual)	☐	☐
7	**Management and Governance Services**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.1	**Logging and Monitoring**		
7.1.1	**Configuring Diagnostic Settings**		
7.1.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs (Manual)	☐	☐
7.1.1.2	Ensure Diagnostic Setting captures appropriate categories (Automated)	☐	☐
7.1.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK) (Automated)	☐	☐
7.1.1.4	Ensure that logging for Azure Key Vault is 'Enabled' (Automated)	☐	☐
7.1.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual)	☐	☐
7.1.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled (Automated)	☐	☐
7.1.1.7	Ensure that virtual network flow logs are captured and sent to Log Analytics (Manual)	☐	☐
7.1.1.8	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination (Manual)	☐	☐
7.1.1.9	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination (Manual)	☐	☐
7.1.1.10	Ensure that Intune logs are captured and sent to Log Analytics (Manual)	☐	☐
7.1.2	**Monitoring using Activity Log Alerts**		
7.1.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.1.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)	☐	☐
7.1.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)	☐	☐
7.1.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)	☐	☐
7.1.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)	☐	☐
7.1.2.6	Ensure that Activity Log Alert exists for Delete Security Solution (Automated)	☐	☐
7.1.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated)	☐	☐
7.1.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated)	☐	☐
7.1.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated)	☐	☐
7.1.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated)	☐	☐
7.1.2.11	Ensure that an Activity Log Alert exists for Service Health (Automated)	☐	☐
7.1.3	**Configuring Application Insights**		
7.1.3.1	Ensure Application Insights are Configured (Automated)	☐	☐
7.1.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)	☐	☐
7.1.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.2	Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual)	☐	☐
8	**Networking Services**		
8.1	Ensure that RDP access from the Internet is evaluated and restricted (Automated)	☐	☐
8.2	Ensure that SSH access from the Internet is evaluated and restricted (Automated)	☐	☐
8.3	Ensure that UDP access from the Internet is evaluated and restricted (Automated)	☐	☐
8.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated)	☐	☐
8.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)	☐	☐
8.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use (Automated)	☐	☐
8.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual)	☐	☐
8.8	Ensure that virtual network flow log retention days is set to greater than or equal to 90 (Automated)	☐	☐
9	**Security Services**		
9.1	**Microsoft Defender for Cloud**		
9.1.1	**Microsoft Cloud Security Posture Management (CSPM)**		
9.1.2	**Defender Plan: APIs**		
9.1.3	**Defender Plan: Servers**		
9.1.3.1	Ensure that Defender for Servers is set to 'On' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On' (Manual)	☐	☐
9.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On' (Manual)	☐	☐
9.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On' (Manual)	☐	☐
9.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On' (Manual)	☐	☐
9.1.4	**Defender Plan: Containers**		
9.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On' (Automated)	☐	☐
9.1.5	**Defender Plan: Storage**		
9.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On' (Automated)	☐	☐
9.1.6	**Defender Plan: App Service**		
9.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On' (Automated)	☐	☐
9.1.7	**Defender Plan: Databases**		
9.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Automated)	☐	☐
9.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Automated)	☐	☐
9.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On' (Automated)	☐	☐
9.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Automated)	☐	☐
9.1.8	**Defender Plan: Key Vault**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Automated)	☐	☐
9.1.9	**Defender Plan: Resource Manager**		
9.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Automated)	☐	☐
9.1.10	Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates (Automated)	☐	☐
9.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' (Manual)	☐	☐
9.1.12	Ensure That 'All users with the following roles' is set to 'Owner' (Automated)	☐	☐
9.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email (Automated)	☐	☐
9.1.14	Ensure that 'Notify about alerts with the following severity (or higher)' is enabled (Automated)	☐	☐
9.1.15	Ensure that 'Notify about attack paths with the following risk level (or higher)' is enabled (Automated)	☐	☐
9.1.16	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled (Manual)	☐	☐
9.1.17	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On' (Automated)	☐	☐
9.2	**Microsoft Defender for IoT**		
9.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On' (Manual)	☐	☐
9.3	**Key Vault**		
9.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated)	☐	☐
9.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated)	☐	☐
9.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated)	☐	☐
9.3.5	Ensure the Key Vault is Recoverable (Automated)	☐	☐
9.3.6	Ensure that Role Based Access Control for Azure Key Vault is enabled (Automated)	☐	☐
9.3.7	Ensure that Public Network Access when using Private Endpoint is disabled (Automated)	☐	☐
9.3.8	Ensure that Private Endpoints are Used for Azure Key Vault (Automated)	☐	☐
9.3.9	Ensure automatic key rotation is enabled within Azure Key Vault (Automated)	☐	☐
9.3.10	Ensure that Azure Key Vault Managed HSM is used when required (Manual)	☐	☐
9.4	**Azure Bastion**		
9.4.1	Ensure an Azure Bastion Host Exists (Automated)	☐	☐
10	**Storage Services**		
10.1	**Azure Files**		
10.1.1	Ensure soft delete for Azure File Shares is Enabled (Automated)	☐	☐
10.1.2	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares (Automated)	☐	☐
10.1.3	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
10.2	**Azure Blob Storage**		
10.2.1	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled (Automated)	☐	☐
10.2.2	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts (Automated)	☐	☐
10.3	**Storage Accounts**		
10.3.1	**Secrets and Keys**		
10.3.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)	☐	☐
10.3.1.2	Ensure that Storage Account access keys are periodically regenerated (Manual)	☐	☐
10.3.1.3	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled' (Automated)	☐	☐
10.3.2	**Networking**		
10.3.2.1	Ensure Private Endpoints are used to access Storage Accounts (Automated)	☐	☐
10.3.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts (Automated)	☐	☐
10.3.2.3	Ensure default network access rule for storage accounts is set to deny (Automated)	☐	☐
10.3.3	**Identity and Access Management**		
10.3.3.1	Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled' (Automated)	☐	☐
10.3.4	Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
10.3.5	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated)	☐	☐
10.3.6	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)	☐	☐
10.3.7	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2' (Automated)	☐	☐
10.3.8	Ensure 'Cross Tenant Replication' is not enabled (Automated)	☐	☐
10.3.9	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled' (Automated)	☐	☐
10.3.10	Ensure Azure Resource Manager Delete locks are applied to Azure Storage Accounts (Manual)	☐	☐
10.3.11	Ensure Azure Resource Manager ReadOnly locks are considered for Azure Storage Accounts (Manual)	☐	☐
10.3.12	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1.2	Ensure that network security groups are configured for Databricks subnets	☐	☐
3.1.7	Ensure that diagnostic log delivery is configured for Azure Databricks	☐	☐
6.1.1	Ensure that 'security defaults' is enabled in Microsoft Entra ID	☐	☐
6.2.2	Ensure that an exclusionary geographic Conditional Access policy is considered	☐	☐
6.2.3	Ensure that an exclusionary device code flow policy is considered	☐	☐
6.3.1	Ensure that Azure admin accounts are not used for daily operations	☐	☐
6.3.2	Ensure that guest users are reviewed on a regular basis	☐	☐
6.4	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	☐	☐
6.12	Ensure that 'User consent for applications' is set to 'Do not allow user consent'	☐	☐
6.13	Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions'	☐	☐
6.14	Ensure that 'Users can register applications' is set to 'No'	☐	☐
6.15	Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	☐	☐
6.17	Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes'	☐	☐
6.18	Ensure that 'Restrict user ability to access groups features in My Groups' is set to 'Yes'	☐	☐
6.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	☐	☐
6.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐
6.24	Ensure that a custom role is assigned permissions for administering resource locks	☐	☐
6.25	Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one'	☐	☐
7.1.1.8	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination	☐	☐
7.1.1.9	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination	☐	☐
7.1.1.10	Ensure that Intune logs are captured and sent to Log Analytics	☐	☐
7.1.3.1	Ensure Application Insights are Configured	☐	☐
7.1.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	☐	☐
7.2	Ensure that Resource Locks are set for Mission-Critical Azure Resources	☐	☐
8.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	☐	☐
8.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	☐	☐
9.1.10	Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates	☐	☐
9.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	☐	☐
9.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	☐	☐
9.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	☐	☐
9.3.5	Ensure the Key Vault is Recoverable	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.3.6	Ensure that Role Based Access Control for Azure Key Vault is enabled	☐	☐
9.3.7	Ensure that Public Network Access when using Private Endpoint is disabled	☐	☐
10.1.1	Ensure soft delete for Azure File Shares is Enabled	☐	☐
10.2.1	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	☐	☐
10.2.2	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	☐	☐
10.3.1.3	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	☐	☐
10.3.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	☐	☐
10.3.3.1	Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled'	☐	☐
10.3.6	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	☐	☐
10.3.9	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1.1	Ensure that Azure Databricks is deployed in a customer-managed virtual network (VNet)	☐	☐
3.1.2	Ensure that network security groups are configured for Databricks subnets	☐	☐
3.1.3	Ensure that traffic is encrypted between cluster worker nodes	☐	☐
3.1.4	Ensure that users and groups are synced from Microsoft Entra ID to Azure Databricks	☐	☐
3.1.5	Ensure that Unity Catalog is configured for Azure Databricks	☐	☐
3.1.6	Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens	☐	☐
3.1.7	Ensure that diagnostic log delivery is configured for Azure Databricks	☐	☐
3.1.8	Ensure that data at rest and in transit is encrypted in Azure Databricks using customer managed keys (CMK)	☐	☐
4.1.1	Ensure only MFA enabled identities can access privileged Virtual Machine	☐	☐
6.1.1	Ensure that 'security defaults' is enabled in Microsoft Entra ID	☐	☐
6.1.2	Ensure that 'multifactor authentication' is 'enabled' for all users	☐	☐
6.1.3	Ensure that 'Allow users to remember multifactor authentication on devices they trust' is disabled	☐	☐
6.2.1	Ensure that 'trusted locations' are defined	☐	☐
6.2.2	Ensure that an exclusionary geographic Conditional Access policy is considered	☐	☐
6.2.3	Ensure that an exclusionary device code flow policy is considered	☐	☐
6.2.4	Ensure that a multifactor authentication policy exists for all users	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.5	Ensure that multifactor authentication is required for risky sign-ins	☐	☐
6.2.6	Ensure that multifactor authentication is required for Windows Azure Service Management API	☐	☐
6.2.7	Ensure that multifactor authentication is required to access Microsoft Admin Portals	☐	☐
6.3.1	Ensure that Azure admin accounts are not used for daily operations	☐	☐
6.3.2	Ensure that guest users are reviewed on a regular basis	☐	☐
6.3.3	Ensure that use of the 'User Access Administrator' role is restricted	☐	☐
6.3.4	Ensure that all 'privileged' role assignments are periodically reviewed	☐	☐
6.4	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	☐	☐
6.5	Ensure that 'Number of methods required to reset' is set to '2'	☐	☐
6.8	Ensure that a 'Custom banned password list' is set to 'Enforce'	☐	☐
6.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	☐	☐
6.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	☐	☐
6.11	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'	☐	☐
6.12	Ensure that 'User consent for applications' is set to 'Do not allow user consent'	☐	☐
6.13	Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions'	☐	☐
6.14	Ensure that 'Users can register applications' is set to 'No'	☐	☐
6.15	Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	☐	☐
6.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.17	Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes'	☐	☐
6.18	Ensure that 'Restrict user ability to access groups features in My Groups' is set to 'Yes'	☐	☐
6.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐
6.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	☐	☐
6.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐
6.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	☐	☐
6.23	Ensure that no custom subscription administrator roles exist	☐	☐
6.24	Ensure that a custom role is assigned permissions for administering resource locks	☐	☐
6.25	Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one'	☐	☐
6.26	Ensure fewer than 5 users have global administrator assignment	☐	☐
7.1.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	☐	☐
7.1.1.2	Ensure Diagnostic Setting captures appropriate categories	☐	☐
7.1.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	☐	☐
7.1.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	☐	☐
7.1.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	☐	☐
7.1.1.7	Ensure that virtual network flow logs are captured and sent to Log Analytics	☐	☐
7.1.1.8	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.1.1.9	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination	☐	☐
7.1.1.10	Ensure that Intune logs are captured and sent to Log Analytics	☐	☐
7.1.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	☐	☐
7.1.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	☐	☐
7.1.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	☐	☐
7.1.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	☐	☐
7.1.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	☐	☐
7.1.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	☐	☐
7.1.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	☐	☐
7.1.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	☐	☐
7.1.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	☐	☐
7.1.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	☐	☐
7.1.2.11	Ensure that an Activity Log Alert exists for Service Health	☐	☐
7.1.3.1	Ensure Application Insights are Configured	☐	☐
7.1.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	☐	☐
7.1.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	☐	☐
7.2	Ensure that Resource Locks are set for Mission-Critical Azure Resources	☐	☐
8.1	Ensure that RDP access from the Internet is evaluated and restricted	☐	☐

Recommendation		Set Correctly	
		Yes	No
8.2	Ensure that SSH access from the Internet is evaluated and restricted	☐	☐
8.3	Ensure that UDP access from the Internet is evaluated and restricted	☐	☐
8.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	☐	☐
8.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	☐	☐
8.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	☐	☐
8.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	☐	☐
8.8	Ensure that virtual network flow log retention days is set to greater than or equal to 90	☐	☐
9.1.3.1	Ensure that Defender for Servers is set to 'On'	☐	☐
9.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	☐	☐
9.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	☐	☐
9.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	☐	☐
9.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	☐	☐
9.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	☐	☐
9.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	☐	☐
9.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	☐	☐
9.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	☐	☐
9.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	☐	☐
9.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	☐	☐
9.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	☐	☐
9.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	☐	☐
9.1.10	Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates	☐	☐
9.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	☐	☐
9.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	☐	☐
9.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	☐	☐
9.1.16	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	☐	☐
9.1.17	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	☐	☐
9.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	☐	☐
9.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	☐	☐
9.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	☐	☐
9.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	☐	☐
9.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	☐	☐
9.3.5	Ensure the Key Vault is Recoverable	☐	☐
9.3.6	Ensure that Role Based Access Control for Azure Key Vault is enabled	☐	☐
9.3.7	Ensure that Public Network Access when using Private Endpoint is disabled	☐	☐
9.3.8	Ensure that Private Endpoints are Used for Azure Key Vault	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.3.9	Ensure automatic key rotation is enabled within Azure Key Vault	☐	☐
9.4.1	Ensure an Azure Bastion Host Exists	☐	☐
10.1.1	Ensure soft delete for Azure File Shares is Enabled	☐	☐
10.1.2	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	☐	☐
10.1.3	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	☐	☐
10.2.1	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	☐	☐
10.2.2	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	☐	☐
10.3.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	☐	☐
10.3.1.2	Ensure that Storage Account access keys are periodically regenerated	☐	☐
10.3.1.3	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	☐	☐
10.3.2.1	Ensure Private Endpoints are used to access Storage Accounts	☐	☐
10.3.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	☐	☐
10.3.3.1	Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled'	☐	☐
10.3.4	Ensure that 'Secure transfer required' is set to 'Enabled'	☐	☐
10.3.6	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	☐	☐
10.3.7	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	☐	☐
10.3.8	Ensure 'Cross Tenant Replication' is not enabled	☐	☐
10.3.9	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1.1	Ensure that Azure Databricks is deployed in a customer-managed virtual network (VNet)	☐	☐
3.1.2	Ensure that network security groups are configured for Databricks subnets	☐	☐
3.1.3	Ensure that traffic is encrypted between cluster worker nodes	☐	☐
3.1.4	Ensure that users and groups are synced from Microsoft Entra ID to Azure Databricks	☐	☐
3.1.5	Ensure that Unity Catalog is configured for Azure Databricks	☐	☐
3.1.6	Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens	☐	☐
3.1.7	Ensure that diagnostic log delivery is configured for Azure Databricks	☐	☐
3.1.8	Ensure that data at rest and in transit is encrypted in Azure Databricks using customer managed keys (CMK)	☐	☐
4.1.1	Ensure only MFA enabled identities can access privileged Virtual Machine	☐	☐
6.1.1	Ensure that 'security defaults' is enabled in Microsoft Entra ID	☐	☐
6.1.2	Ensure that 'multifactor authentication' is 'enabled' for all users	☐	☐
6.1.3	Ensure that 'Allow users to remember multifactor authentication on devices they trust' is disabled	☐	☐
6.2.1	Ensure that 'trusted locations' are defined	☐	☐
6.2.2	Ensure that an exclusionary geographic Conditional Access policy is considered	☐	☐
6.2.3	Ensure that an exclusionary device code flow policy is considered	☐	☐
6.2.4	Ensure that a multifactor authentication policy exists for all users	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.5	Ensure that multifactor authentication is required for risky sign-ins	☐	☐
6.2.6	Ensure that multifactor authentication is required for Windows Azure Service Management API	☐	☐
6.2.7	Ensure that multifactor authentication is required to access Microsoft Admin Portals	☐	☐
6.3.1	Ensure that Azure admin accounts are not used for daily operations	☐	☐
6.3.2	Ensure that guest users are reviewed on a regular basis	☐	☐
6.3.3	Ensure that use of the 'User Access Administrator' role is restricted	☐	☐
6.3.4	Ensure that all 'privileged' role assignments are periodically reviewed	☐	☐
6.4	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	☐	☐
6.5	Ensure that 'Number of methods required to reset' is set to '2'	☐	☐
6.8	Ensure that a 'Custom banned password list' is set to 'Enforce'	☐	☐
6.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	☐	☐
6.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	☐	☐
6.11	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'	☐	☐
6.12	Ensure that 'User consent for applications' is set to 'Do not allow user consent'	☐	☐
6.13	Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions'	☐	☐
6.14	Ensure that 'Users can register applications' is set to 'No'	☐	☐
6.15	Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	☐	☐
6.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.17	Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes'	☐	☐
6.18	Ensure that 'Restrict user ability to access groups features in My Groups' is set to 'Yes'	☐	☐
6.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐
6.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	☐	☐
6.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐
6.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	☐	☐
6.23	Ensure that no custom subscription administrator roles exist	☐	☐
6.24	Ensure that a custom role is assigned permissions for administering resource locks	☐	☐
6.25	Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one'	☐	☐
6.26	Ensure fewer than 5 users have global administrator assignment	☐	☐
7.1.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	☐	☐
7.1.1.2	Ensure Diagnostic Setting captures appropriate categories	☐	☐
7.1.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK)	☐	☐
7.1.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	☐	☐
7.1.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	☐	☐
7.1.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	☐	☐
7.1.1.7	Ensure that virtual network flow logs are captured and sent to Log Analytics	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.1.1.8	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination	☐	☐
7.1.1.9	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination	☐	☐
7.1.1.10	Ensure that Intune logs are captured and sent to Log Analytics	☐	☐
7.1.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	☐	☐
7.1.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	☐	☐
7.1.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	☐	☐
7.1.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	☐	☐
7.1.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	☐	☐
7.1.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	☐	☐
7.1.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	☐	☐
7.1.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	☐	☐
7.1.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	☐	☐
7.1.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	☐	☐
7.1.2.11	Ensure that an Activity Log Alert exists for Service Health	☐	☐
7.1.3.1	Ensure Application Insights are Configured	☐	☐
7.1.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	☐	☐
7.1.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.2	Ensure that Resource Locks are set for Mission-Critical Azure Resources	☐	☐
8.1	Ensure that RDP access from the Internet is evaluated and restricted	☐	☐
8.2	Ensure that SSH access from the Internet is evaluated and restricted	☐	☐
8.3	Ensure that UDP access from the Internet is evaluated and restricted	☐	☐
8.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	☐	☐
8.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	☐	☐
8.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	☐	☐
8.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	☐	☐
8.8	Ensure that virtual network flow log retention days is set to greater than or equal to 90	☐	☐
9.1.3.1	Ensure that Defender for Servers is set to 'On'	☐	☐
9.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	☐	☐
9.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	☐	☐
9.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	☐	☐
9.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	☐	☐
9.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	☐	☐
9.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	☐	☐
9.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	☐	☐
9.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	☐	☐
9.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	☐	☐
9.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	☐	☐
9.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	☐	☐
9.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	☐	☐
9.1.10	Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates	☐	☐
9.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	☐	☐
9.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	☐	☐
9.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	☐	☐
9.1.14	Ensure that 'Notify about alerts with the following severity (or higher)' is enabled	☐	☐
9.1.15	Ensure that 'Notify about attack paths with the following risk level (or higher)' is enabled	☐	☐
9.1.16	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	☐	☐
9.1.17	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	☐	☐
9.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	☐	☐
9.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	☐	☐
9.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	☐	☐
9.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	☐	☐
9.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.3.5	Ensure the Key Vault is Recoverable	☐	☐
9.3.6	Ensure that Role Based Access Control for Azure Key Vault is enabled	☐	☐
9.3.7	Ensure that Public Network Access when using Private Endpoint is disabled	☐	☐
9.3.8	Ensure that Private Endpoints are Used for Azure Key Vault	☐	☐
9.3.9	Ensure automatic key rotation is enabled within Azure Key Vault	☐	☐
9.3.10	Ensure that Azure Key Vault Managed HSM is used when required	☐	☐
9.4.1	Ensure an Azure Bastion Host Exists	☐	☐
10.1.1	Ensure soft delete for Azure File Shares is Enabled	☐	☐
10.1.2	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	☐	☐
10.1.3	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	☐	☐
10.2.1	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	☐	☐
10.2.2	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	☐	☐
10.3.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	☐	☐
10.3.1.2	Ensure that Storage Account access keys are periodically regenerated	☐	☐
10.3.1.3	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	☐	☐
10.3.2.1	Ensure Private Endpoints are used to access Storage Accounts	☐	☐
10.3.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	☐	☐
10.3.2.3	Ensure default network access rule for storage accounts is set to deny	☐	☐
10.3.3.1	Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled'	☐	☐

Recommendation		Set Correctly	
		Yes	No
10.3.4	Ensure that 'Secure transfer required' is set to 'Enabled'	☐	☐
10.3.5	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	☐	☐
10.3.6	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	☐	☐
10.3.7	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	☐	☐
10.3.8	Ensure 'Cross Tenant Replication' is not enabled	☐	☐
10.3.9	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
6.6	Ensure that account 'Lockout threshold' is less than or equal to '10'	☐	☐
6.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60'	☐	☐
10.3.10	Ensure Azure Resource Manager Delete locks are applied to Azure Storage Accounts	☐	☐
10.3.11	Ensure Azure Resource Manager ReadOnly locks are considered for Azure Storage Accounts	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1.2	Ensure that network security groups are configured for Databricks subnets	☐	☐
3.1.6	Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens	☐	☐
3.1.7	Ensure that diagnostic log delivery is configured for Azure Databricks	☐	☐
4.1.1	Ensure only MFA enabled identities can access privileged Virtual Machine	☐	☐
6.1.1	Ensure that 'security defaults' is enabled in Microsoft Entra ID	☐	☐
6.1.2	Ensure that 'multifactor authentication' is 'enabled' for all users	☐	☐
6.1.3	Ensure that 'Allow users to remember multifactor authentication on devices they trust' is disabled	☐	☐
6.2.3	Ensure that an exclusionary device code flow policy is considered	☐	☐
6.2.4	Ensure that a multifactor authentication policy exists for all users	☐	☐
6.2.5	Ensure that multifactor authentication is required for risky sign-ins	☐	☐
6.2.6	Ensure that multifactor authentication is required for Windows Azure Service Management API	☐	☐
6.2.7	Ensure that multifactor authentication is required to access Microsoft Admin Portals	☐	☐
6.3.1	Ensure that Azure admin accounts are not used for daily operations	☐	☐
6.3.2	Ensure that guest users are reviewed on a regular basis	☐	☐
6.5	Ensure that 'Number of methods required to reset' is set to '2'	☐	☐
6.8	Ensure that a 'Custom banned password list' is set to 'Enforce'	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	☐	☐
6.11	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'	☐	☐
6.12	Ensure that 'User consent for applications' is set to 'Do not allow user consent'	☐	☐
6.13	Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions'	☐	☐
6.14	Ensure that 'Users can register applications' is set to 'No'	☐	☐
6.15	Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	☐	☐
6.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	☐	☐
6.17	Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes'	☐	☐
6.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	☐	☐
6.23	Ensure that no custom subscription administrator roles exist	☐	☐
6.24	Ensure that a custom role is assigned permissions for administering resource locks	☐	☐
6.25	Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one'	☐	☐
6.26	Ensure fewer than 5 users have global administrator assignment	☐	☐
7.1.1.8	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination	☐	☐
7.1.1.9	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination	☐	☐
7.1.1.10	Ensure that Intune logs are captured and sent to Log Analytics	☐	☐
7.1.3.1	Ensure Application Insights are Configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.1.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	☐	☐
7.2	Ensure that Resource Locks are set for Mission-Critical Azure Resources	☐	☐
8.2	Ensure that SSH access from the Internet is evaluated and restricted	☐	☐
8.3	Ensure that UDP access from the Internet is evaluated and restricted	☐	☐
8.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	☐	☐
8.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	☐	☐
8.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	☐	☐
8.8	Ensure that virtual network flow log retention days is set to greater than or equal to 90	☐	☐
9.1.3.1	Ensure that Defender for Servers is set to 'On'	☐	☐
9.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	☐	☐
9.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	☐	☐
9.1.10	Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates	☐	☐
9.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	☐	☐
9.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	☐	☐
9.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	☐	☐
9.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	☐	☐
9.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	☐	☐
9.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	☐	☐
9.3.5	Ensure the Key Vault is Recoverable	☐	☐
9.3.6	Ensure that Role Based Access Control for Azure Key Vault is enabled	☐	☐
9.3.7	Ensure that Public Network Access when using Private Endpoint is disabled	☐	☐
9.3.9	Ensure automatic key rotation is enabled within Azure Key Vault	☐	☐
9.4.1	Ensure an Azure Bastion Host Exists	☐	☐
10.1.1	Ensure soft delete for Azure File Shares is Enabled	☐	☐
10.2.1	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	☐	☐
10.2.2	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	☐	☐
10.3.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	☐	☐
10.3.1.2	Ensure that Storage Account access keys are periodically regenerated	☐	☐
10.3.1.3	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	☐	☐
10.3.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	☐	☐
10.3.3.1	Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled'	☐	☐
10.3.5	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	☐	☐
10.3.6	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	☐	☐
10.3.8	Ensure 'Cross Tenant Replication' is not enabled	☐	☐
10.3.9	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	☐	☐
10.3.12	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1.1	Ensure that Azure Databricks is deployed in a customer-managed virtual network (VNet)	☐	☐
3.1.2	Ensure that network security groups are configured for Databricks subnets	☐	☐
3.1.3	Ensure that traffic is encrypted between cluster worker nodes	☐	☐
3.1.4	Ensure that users and groups are synced from Microsoft Entra ID to Azure Databricks	☐	☐
3.1.5	Ensure that Unity Catalog is configured for Azure Databricks	☐	☐
3.1.6	Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens	☐	☐
3.1.7	Ensure that diagnostic log delivery is configured for Azure Databricks	☐	☐
3.1.8	Ensure that data at rest and in transit is encrypted in Azure Databricks using customer managed keys (CMK)	☐	☐
4.1.1	Ensure only MFA enabled identities can access privileged Virtual Machine	☐	☐
6.1.1	Ensure that 'security defaults' is enabled in Microsoft Entra ID	☐	☐
6.1.2	Ensure that 'multifactor authentication' is 'enabled' for all users	☐	☐
6.1.3	Ensure that 'Allow users to remember multifactor authentication on devices they trust' is disabled	☐	☐
6.2.1	Ensure that 'trusted locations' are defined	☐	☐
6.2.2	Ensure that an exclusionary geographic Conditional Access policy is considered	☐	☐
6.2.3	Ensure that an exclusionary device code flow policy is considered	☐	☐
6.2.4	Ensure that a multifactor authentication policy exists for all users	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.5	Ensure that multifactor authentication is required for risky sign-ins	☐	☐
6.2.6	Ensure that multifactor authentication is required for Windows Azure Service Management API	☐	☐
6.2.7	Ensure that multifactor authentication is required to access Microsoft Admin Portals	☐	☐
6.3.1	Ensure that Azure admin accounts are not used for daily operations	☐	☐
6.3.2	Ensure that guest users are reviewed on a regular basis	☐	☐
6.5	Ensure that 'Number of methods required to reset' is set to '2'	☐	☐
6.6	Ensure that account 'Lockout threshold' is less than or equal to '10'	☐	☐
6.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60'	☐	☐
6.8	Ensure that a 'Custom banned password list' is set to 'Enforce'	☐	☐
6.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	☐	☐
6.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	☐	☐
6.11	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'	☐	☐
6.12	Ensure that 'User consent for applications' is set to 'Do not allow user consent'	☐	☐
6.13	Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions'	☐	☐
6.14	Ensure that 'Users can register applications' is set to 'No'	☐	☐
6.15	Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	☐	☐
6.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	☐	☐
6.17	Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes'	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	☐	☐
6.23	Ensure that no custom subscription administrator roles exist	☐	☐
6.24	Ensure that a custom role is assigned permissions for administering resource locks	☐	☐
6.25	Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one'	☐	☐
6.26	Ensure fewer than 5 users have global administrator assignment	☐	☐
7.1.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	☐	☐
7.1.1.2	Ensure Diagnostic Setting captures appropriate categories	☐	☐
7.1.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK)	☐	☐
7.1.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	☐	☐
7.1.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	☐	☐
7.1.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	☐	☐
7.1.1.7	Ensure that virtual network flow logs are captured and sent to Log Analytics	☐	☐
7.1.1.8	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination	☐	☐
7.1.1.9	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination	☐	☐
7.1.1.10	Ensure that Intune logs are captured and sent to Log Analytics	☐	☐
7.1.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	☐	☐
7.1.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.1.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	☐	☐
7.1.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	☐	☐
7.1.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	☐	☐
7.1.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	☐	☐
7.1.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	☐	☐
7.1.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	☐	☐
7.1.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	☐	☐
7.1.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	☐	☐
7.1.2.11	Ensure that an Activity Log Alert exists for Service Health	☐	☐
7.1.3.1	Ensure Application Insights are Configured	☐	☐
7.1.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	☐	☐
7.1.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	☐	☐
7.2	Ensure that Resource Locks are set for Mission-Critical Azure Resources	☐	☐
8.1	Ensure that RDP access from the Internet is evaluated and restricted	☐	☐
8.2	Ensure that SSH access from the Internet is evaluated and restricted	☐	☐
8.3	Ensure that UDP access from the Internet is evaluated and restricted	☐	☐
8.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	☐	☐
8.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	☐	☐

Recommendation		Set Correctly	
		Yes	No
8.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	☐	☐
8.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	☐	☐
8.8	Ensure that virtual network flow log retention days is set to greater than or equal to 90	☐	☐
9.1.3.1	Ensure that Defender for Servers is set to 'On'	☐	☐
9.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	☐	☐
9.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	☐	☐
9.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	☐	☐
9.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	☐	☐
9.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	☐	☐
9.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	☐	☐
9.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	☐	☐
9.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	☐	☐
9.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	☐	☐
9.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	☐	☐
9.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	☐	☐
9.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	☐	☐
9.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	☐	☐
9.1.10	Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	☐	☐
9.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	☐	☐
9.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	☐	☐
9.1.16	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	☐	☐
9.1.17	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	☐	☐
9.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	☐	☐
9.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	☐	☐
9.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	☐	☐
9.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	☐	☐
9.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	☐	☐
9.3.5	Ensure the Key Vault is Recoverable	☐	☐
9.3.6	Ensure that Role Based Access Control for Azure Key Vault is enabled	☐	☐
9.3.7	Ensure that Public Network Access when using Private Endpoint is disabled	☐	☐
9.3.8	Ensure that Private Endpoints are Used for Azure Key Vault	☐	☐
9.3.9	Ensure automatic key rotation is enabled within Azure Key Vault	☐	☐
9.3.10	Ensure that Azure Key Vault Managed HSM is used when required	☐	☐
9.4.1	Ensure an Azure Bastion Host Exists	☐	☐
10.1.1	Ensure soft delete for Azure File Shares is Enabled	☐	☐
10.1.2	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	☐	☐

Recommendation		Set Correctly	
		Yes	No
10.1.3	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	☐	☐
10.2.1	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	☐	☐
10.2.2	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	☐	☐
10.3.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	☐	☐
10.3.1.2	Ensure that Storage Account access keys are periodically regenerated	☐	☐
10.3.1.3	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	☐	☐
10.3.2.1	Ensure Private Endpoints are used to access Storage Accounts	☐	☐
10.3.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	☐	☐
10.3.2.3	Ensure default network access rule for storage accounts is set to deny	☐	☐
10.3.3.1	Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled'	☐	☐
10.3.4	Ensure that 'Secure transfer required' is set to 'Enabled'	☐	☐
10.3.5	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	☐	☐
10.3.6	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	☐	☐
10.3.7	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	☐	☐
10.3.8	Ensure 'Cross Tenant Replication' is not enabled	☐	☐
10.3.9	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	☐	☐
10.3.12	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1.1	Ensure that Azure Databricks is deployed in a customer-managed virtual network (VNet)	☐	☐
3.1.2	Ensure that network security groups are configured for Databricks subnets	☐	☐
3.1.3	Ensure that traffic is encrypted between cluster worker nodes	☐	☐
3.1.4	Ensure that users and groups are synced from Microsoft Entra ID to Azure Databricks	☐	☐
3.1.5	Ensure that Unity Catalog is configured for Azure Databricks	☐	☐
3.1.6	Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens	☐	☐
3.1.7	Ensure that diagnostic log delivery is configured for Azure Databricks	☐	☐
3.1.8	Ensure that data at rest and in transit is encrypted in Azure Databricks using customer managed keys (CMK)	☐	☐
4.1.1	Ensure only MFA enabled identities can access privileged Virtual Machine	☐	☐
6.1.1	Ensure that 'security defaults' is enabled in Microsoft Entra ID	☐	☐
6.1.2	Ensure that 'multifactor authentication' is 'enabled' for all users	☐	☐
6.1.3	Ensure that 'Allow users to remember multifactor authentication on devices they trust' is disabled	☐	☐
6.2.1	Ensure that 'trusted locations' are defined	☐	☐
6.2.2	Ensure that an exclusionary geographic Conditional Access policy is considered	☐	☐
6.2.3	Ensure that an exclusionary device code flow policy is considered	☐	☐
6.2.4	Ensure that a multifactor authentication policy exists for all users	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.5	Ensure that multifactor authentication is required for risky sign-ins	☐	☐
6.2.6	Ensure that multifactor authentication is required for Windows Azure Service Management API	☐	☐
6.2.7	Ensure that multifactor authentication is required to access Microsoft Admin Portals	☐	☐
6.3.1	Ensure that Azure admin accounts are not used for daily operations	☐	☐
6.3.2	Ensure that guest users are reviewed on a regular basis	☐	☐
6.3.3	Ensure that use of the 'User Access Administrator' role is restricted	☐	☐
6.3.4	Ensure that all 'privileged' role assignments are periodically reviewed	☐	☐
6.4	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	☐	☐
6.5	Ensure that 'Number of methods required to reset' is set to '2'	☐	☐
6.6	Ensure that account 'Lockout threshold' is less than or equal to '10'	☐	☐
6.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60'	☐	☐
6.8	Ensure that a 'Custom banned password list' is set to 'Enforce'	☐	☐
6.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	☐	☐
6.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	☐	☐
6.11	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'	☐	☐
6.12	Ensure that 'User consent for applications' is set to 'Do not allow user consent'	☐	☐
6.13	Ensure that 'User consent for applications' is set to 'Allow user consent for apps from verified publishers, for selected permissions'	☐	☐
6.14	Ensure that 'Users can register applications' is set to 'No'	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.15	Ensure that 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	☐	☐
6.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	☐	☐
6.17	Ensure that 'Restrict access to Microsoft Entra admin center' is set to 'Yes'	☐	☐
6.18	Ensure that 'Restrict user ability to access groups features in My Groups' is set to 'Yes'	☐	☐
6.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐
6.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	☐	☐
6.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	☐	☐
6.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	☐	☐
6.23	Ensure that no custom subscription administrator roles exist	☐	☐
6.24	Ensure that a custom role is assigned permissions for administering resource locks	☐	☐
6.25	Ensure that 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' is set to 'Permit no one'	☐	☐
6.26	Ensure fewer than 5 users have global administrator assignment	☐	☐
7.1.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	☐	☐
7.1.1.2	Ensure Diagnostic Setting captures appropriate categories	☐	☐
7.1.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK)	☐	☐
7.1.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	☐	☐
7.1.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.1.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	☐	☐
7.1.1.7	Ensure that virtual network flow logs are captured and sent to Log Analytics	☐	☐
7.1.1.8	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination	☐	☐
7.1.1.9	Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination	☐	☐
7.1.1.10	Ensure that Intune logs are captured and sent to Log Analytics	☐	☐
7.1.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	☐	☐
7.1.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	☐	☐
7.1.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	☐	☐
7.1.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	☐	☐
7.1.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	☐	☐
7.1.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	☐	☐
7.1.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	☐	☐
7.1.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	☐	☐
7.1.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	☐	☐
7.1.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	☐	☐
7.1.2.11	Ensure that an Activity Log Alert exists for Service Health	☐	☐
7.1.3.1	Ensure Application Insights are Configured	☐	☐
7.1.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	☐	☐

Recommendation		Set Correctly	
		Yes	No
7.1.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	☐	☐
7.2	Ensure that Resource Locks are set for Mission-Critical Azure Resources	☐	☐
8.1	Ensure that RDP access from the Internet is evaluated and restricted	☐	☐
8.2	Ensure that SSH access from the Internet is evaluated and restricted	☐	☐
8.3	Ensure that UDP access from the Internet is evaluated and restricted	☐	☐
8.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	☐	☐
8.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	☐	☐
8.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	☐	☐
8.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	☐	☐
8.8	Ensure that virtual network flow log retention days is set to greater than or equal to 90	☐	☐
9.1.3.1	Ensure that Defender for Servers is set to 'On'	☐	☐
9.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	☐	☐
9.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	☐	☐
9.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	☐	☐
9.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	☐	☐
9.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	☐	☐
9.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	☐	☐
9.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	☐	☐
9.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	☐	☐
9.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	☐	☐
9.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	☐	☐
9.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	☐	☐
9.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	☐	☐
9.1.10	Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates	☐	☐
9.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	☐	☐
9.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	☐	☐
9.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	☐	☐
9.1.14	Ensure that 'Notify about alerts with the following severity (or higher)' is enabled	☐	☐
9.1.15	Ensure that 'Notify about attack paths with the following risk level (or higher)' is enabled	☐	☐
9.1.16	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	☐	☐
9.1.17	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	☐	☐
9.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	☐	☐
9.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	☐	☐
9.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	☐	☐
9.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	☐	☐

Recommendation		Set Correctly	
		Yes	No
9.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	☐	☐
9.3.5	Ensure the Key Vault is Recoverable	☐	☐
9.3.6	Ensure that Role Based Access Control for Azure Key Vault is enabled	☐	☐
9.3.7	Ensure that Public Network Access when using Private Endpoint is disabled	☐	☐
9.3.8	Ensure that Private Endpoints are Used for Azure Key Vault	☐	☐
9.3.9	Ensure automatic key rotation is enabled within Azure Key Vault	☐	☐
9.3.10	Ensure that Azure Key Vault Managed HSM is used when required	☐	☐
9.4.1	Ensure an Azure Bastion Host Exists	☐	☐
10.1.1	Ensure soft delete for Azure File Shares is Enabled	☐	☐
10.1.2	Ensure 'SMB protocol version' is set to 'SMB 3.1.1' or higher for SMB file shares	☐	☐
10.1.3	Ensure 'SMB channel encryption' is set to 'AES-256-GCM' or higher for SMB file shares	☐	☐
10.2.1	Ensure that soft delete for blobs on Azure Blob Storage storage accounts is Enabled	☐	☐
10.2.2	Ensure 'Versioning' is set to 'Enabled' on Azure Blob Storage storage accounts	☐	☐
10.3.1.1	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	☐	☐
10.3.1.2	Ensure that Storage Account access keys are periodically regenerated	☐	☐
10.3.1.3	Ensure 'Allow storage account key access' for Azure Storage Accounts is 'Disabled'	☐	☐
10.3.2.1	Ensure Private Endpoints are used to access Storage Accounts	☐	☐
10.3.2.2	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	☐	☐
10.3.2.3	Ensure default network access rule for storage accounts is set to deny	☐	☐

Recommendation		Set Correctly	
		Yes	No
10.3.3.1	Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled'	☐	☐
10.3.4	Ensure that 'Secure transfer required' is set to 'Enabled'	☐	☐
10.3.5	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	☐	☐
10.3.6	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	☐	☐
10.3.7	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	☐	☐
10.3.8	Ensure 'Cross Tenant Replication' is not enabled	☐	☐
10.3.9	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	☐	☐
10.3.12	Ensure Redundancy is set to 'geo-redundant storage (GRS)' on critical Azure Storage Accounts	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	☐	☐

Appendix: Change History

Date	Version	Changes for this version
23-Mar-25	4.0.0	ADD - Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Entra activity logs to an appropriate destination (Ticket 24299)
14-Mar-25	4.0.0	ADD - Ensure that a Microsoft Entra diagnostic setting exists to send Microsoft Graph activity logs to an appropriate destination (Ticket 20484)
12-Mar-25	4.0.0	ADD - Ensure that Azure admin accounts are not used for daily operations (Ticket 22179)
23-Mar-25	4.0.0	ADD - Ensure that Azure Databricks is deployed in a customer-managed virtual network (VNet) (Ticket 24302)
5-Mar-25	4.0.0	ADD - Ensure that Azure Key Vault Managed HSM is used when required (Ticket 17196)
23-Mar-25	4.0.0	ADD - Ensure that data at rest and in transit is encrypted in Azure Databricks using customer managed keys (CMK) (Ticket 24312)
23-Mar-25	4.0.0	ADD - Ensure that 'Default to Microsoft Entra authorization in the Azure portal' is set to 'Enabled' (Ticket 20792)
23-Mar-25	4.0.0	ADD - Ensure that diagnostic log delivery is configured for Azure Databricks (Ticket 24311)
5-Mar-25	4.0.0	ADD - Ensure that encryption at host is enabled (Ticket 20793)
23-Mar-25	4.0.0	ADD - Ensure that Intune logs are captured and sent to Log Analytics (Ticket 18602)
23-Mar-25	4.0.0	ADD - Ensure that network security groups are configured for Databricks subnets (Ticket 24303)
14-Mar-25	4.0.0	ADD - Ensure that 'Notify about attack paths with the following risk level (or higher)' is enabled (Ticket 23796)
23-Mar-25	4.0.0	ADD - Ensure that Public Network Access when using Private Endpoint is disabled (Ticket 24314)
23-Mar-25	4.0.0	ADD - Ensure that traffic is encrypted between cluster worker nodes (Ticket 24304)
23-Mar-25	4.0.0	ADD - Ensure that Unity Catalog is configured for Azure Databricks (Ticket 24309)
23-Mar-25	4.0.0	ADD - Ensure that usage is restricted and expiry is enforced for Databricks personal access tokens (Ticket 24310)

5-Mar-25	4.0.0	ADD - Ensure that use of the 'User Access Administrator' role is restricted (Ticket 19007)
23-Mar-25	4.0.0	ADD - Ensure that users and groups are synced from Microsoft Entra ID to Azure Databricks (Ticket 24308)
23-Mar-25	4.0.0	ADD - Ensure that virtual network flow log retention days is set to greater than or equal to 90 (Ticket 24313)
14-Mar-25	4.0.0	ADD - Ensure that virtual network flow logs are captured and sent to Log Analytics (Ticket 22595)
12-Feb-25	4.0.0	DELETE - Ensure that a multifactor authentication policy exists for administrative groups (Ticket 22337)
20-Feb-25	4.0.0	DELETE - Ensure that 'Agentless container vulnerability assessment' component status is 'On' (Ticket 23436)
20-Feb-25	4.0.0	DELETE - Ensure that 'Agentless discovery for Kubernetes' component status 'On' (Ticket 23435)
20-Feb-25	4.0.0	DELETE - Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' (Ticket 22569)
20-Feb-25	4.0.0	DELETE - Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected (Ticket 22726)
10-Feb-25	4.0.0	DELETE - Ensure that 'multifactor authentication' is 'enabled' for all non-privileged users - MFA for privileged accounts is now default, MFA recommendations have merged to 'all users' (Ticket 23810)
23-Mar-25	4.0.0	MOVED - ALL (28 of 28) Database Recommendations to CIS Microsoft Azure Database Services Benchmark (Ticket 24317)
23-Mar-25	4.0.0	MOVED - MOST (29 of 30) Compute Recommendations moved to CIS Microsoft Azure Compute Services Benchmark (Ticket 24316)
23-Mar-25	4.0.0	MOVED - MOST (35 of 56) Storage Recommendations moved to CIS Microsoft Azure Storage Services Benchmark (Ticket 24318)
10-Mar-25	4.0.0	REMOVE - Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’ - Move to Storage Services Benchmark (Ticket 22275)
19-Mar-25	4.0.0	UDPATE - Ensure that Microsoft Defender for Cloud is configured to check VM operating systems for updates - Added policy that checks status of Update Center (Ticket 22062)

4-Feb-25	4.0.0	UPDATE - All Identity Section Recommendations - Recommendation Names Updated for Consistency (Ticket 23344)
6-Mar-25	4.0.0	UPDATE - Ensure an Azure Bastion Host Exists - Update MITRE Mappings (Ticket 22525)
7-Mar-25	4.0.0	UPDATE - Ensure Application Insights are Configured - Update MITRE Mappings (Ticket 22524)
20-Feb-25	4.0.0	UPDATE - Ensure automatic key rotation is enabled within Azure Key Vault - Added rationale to indicate origin of 'two years' maximum key lifetime duration (Ticket 22721)
11-Mar-25	4.0.0	UPDATE - Ensure Azure Key Vaults are Used to Store Secrets - Update Audit from Azure CLI (Ticket 23087)
11-Mar-25	4.0.0	UPDATE - Ensure only MFA enabled identities can access privileged Virtual Machine - Add instructions for Conditional Access (Ticket 22753)
27-Feb-25	4.0.0	UPDATE - Ensure Private Endpoints are used to access Cosmos DB accounts - Add Audit from CLI & PowerShell, Remediate from CLI, Align with Common Reference Recommendation (Ticket 22426)
6-Feb-25	4.0.0	UPDATE - Ensure that a custom role is assigned permissions for administering resource locks - Updated Procedures & Prose (Ticket 22451)
20-Feb-25	4.0.0	UPDATE - Ensure that App Service apps are configured to use managed identities - Nomenclature and language updated (Ticket 23768)
5-Mar-25	4.0.0	UPDATE - Ensure that Defender for Servers is set to 'On' - Update description to specify enabled components (Ticket 22728)
10-Mar-25	4.0.0	UPDATE - Ensure that 'Enable key rotation reminders' is enabled for each Storage Account - Added supportive Azure Policy (Ticket 24135)
6-Mar-25	4.0.0	UPDATE - Ensure that Endpoint Protection for all Virtual Machines is installed - Replace deprecated Azure Policy (Ticket 23642)
13-Mar-25	4.0.0	UPDATE - Ensure that logging for Azure AppService 'HTTP logs' is enabled - Add Policy (Ticket 18601)
20-Feb-25	4.0.0	UPDATE - Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled - Procedures improved (Ticket 22422)

20-Feb-25	4.0.0	UPDATE - Ensure That Microsoft Defender for Containers Is Set To 'On' - Updated to reflect multiple extensions related to the primary product and simplified to one recommendation instead of three (Ticket 21755)
5-Mar-25	4.0.0	UPDATE - Ensure That Microsoft Defender for Storage Is Set To 'On' - Replaced Deprecated Azure Policy (Ticket 23567)
10-Feb-25	4.0.0	UPDATE - Ensure that 'multifactor authentication' is 'enabled' for all users - MFA for privileged accounts is now default, MFA recommendations have merged to 'all users' (Ticket 23809)
11-Mar-25	4.0.0	UPDATE - Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' - Retirement Notice added: NSG Flow Logs to be Deprecated in 2027 (Ticket 23636)
5-Mar-25	4.0.0	UPDATE - Ensure that 'Notify about alerts with the following severity (or higher)' is enabled - Remove severity requirement, add Impact Statement (Ticket 23639)
13-Feb-25	4.0.0	UPDATE - Ensure that 'Public Network Access' is set to 'Selected Networks' - CLI & Powershell updated, Title Updated (Ticket 22425)
14-Mar-25	4.0.0	UPDATE - Ensure that RDP access from the Internet is evaluated and restricted - Added a resource graph query (Ticket 23817)
14-Mar-25	4.0.0	UPDATE - Ensure that RDP access from the Internet is evaluated and restricted - Refine Audit and Remediation Procedures (Ticket 19629)
6-Mar-25	4.0.0	UPDATE - Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) - Add detail to Remediation Procedure (Ticket 22432)
20-Feb-25	4.0.0	UPDATE - Ensure the Key Vault is Recoverable - Removed obsolete policy for soft delete which is checked with existing policy object (Ticket 23589)
27-Feb-25	4.0.0	UPDATE - Ensure the 'Minimum Inbound TLS Version' for apps is set to '1.2' or higher - Prose changed to reflect "1.2 or higher" and policy added to disable TLS 1.0 and 1.1 (Ticket 23033)
27-Feb-25	4.0.0	UPDATE - Ensure Trusted Launch is enabled on Virtual Machines - Add Audit from CLI & PowerShell, Remediate from CLI & PowerShell (Ticket 23089)

27-Feb-25	4.0.0	UPDATE - Ensure Trusted Launch is enabled on Virtual Machines - Update Azure Policy (Ticket 23633)
5-Feb-25	4.0.0	UPDATE - Included Management Group in Audit and Remediation Steps for "Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'" (Ticket 22727)
17-Mar-25	4.0.0	UPDATE - Multiple Methods of Audit and Remediation - Updated Authenticating with PowerShell to use method other than device code (Ticket 24226)
2-Sep-24	4.0.0	UPDATE - Update MySQL Database recommendations to apply to Azure Database for MySQL - Flexible Servers - Updated recommendations to apply to flexible servers (Ticket 22455)
28-Aug-24	3.0.0	ADD - Defender Cloud Security Posture Management - Text Subsection Article, No Recommendations (Ticket 18605)
28-Aug-24	3.0.0	ADD - Defender for API - Subsection Information Article, No Recommendations (Ticket 19125)
26-Aug-24	3.0.0	ADD - Ensure that account 'Lockout duration in seconds' is greater than or equal to '60' (Ticket 22443)
26-Aug-24	3.0.0	ADD - Ensure that account 'Lockout Threshold' is less than or equal to '10' (Ticket 22079)
5-Sep-24	3.0.0	ADD - Ensure that 'Agentless container vulnerability assessment' component status is 'On' (Ticket 22514)
30-Aug-24	3.0.0	ADD - Ensure that 'Agentless scanning for machines' component status is set to 'On' (Ticket 22474)
28-Aug-24	3.0.0	ADD - Ensure that an exclusionary Device code flow policy is considered (Ticket 21071)
19-Aug-24	3.0.0	ADD - Ensure that 'Basic Authentication' is 'Disabled' (Ticket 22383)
26-Aug-24	3.0.0	ADD - Ensure that 'Data Access Authentication Mode' is 'Disabled' (Ticket 20794)
21-Aug-24	3.0.0	ADD - Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Ticket 22400)
30-Aug-24	3.0.0	ADD - Ensure that 'File Integrity Monitoring' component status is set to 'On' (Ticket 22475)
26-Aug-24	3.0.0	ADD - Ensure that 'Remote debugging' is set to 'Off' Draft (Ticket 22419)
16-Aug-24	3.0.0	ADD - Microsoft Cloud Security Posture Management - New Section (Ticket 22207)
16-Aug-24	3.0.0	ADD - Microsoft Defender for APIs - New Section (Ticket 22222)

13-Feb-24	3.0.0	ADDED - Ensure Ensure that `Allow Blob Anonymous Access` is set to `Disabled` (Ticket 20640)
16-Aug-24	3.0.0	DELETE - Ensure that 'Users can add gallery apps to My Apps' is set to 'No' (Ticket 22199)
22-Jan-24	3.0.0	UPDATE - [LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On' - Updated to legacy with description indicating plan change (Ticket 20485)
3-Sep-24	3.0.0	UPDATE - 1.1.1 Ensure Security Defaults is enabled on Microsoft Entra ID Impact Description Update - Clarify that Conditional Access should be used instead if possible (Ticket 22140)
3-Sep-24	3.0.0	UPDATE - Add CLI Audit and Remediation commands and update Assessment Status to Automated - CLI and PowerShell commands added, status changed from manual to automated (Ticket 22423)
3-Sep-24	3.0.0	UPDATE - Add CLI Audit and Remediation commands and update Assessment Status to Automated - CLI and PowerShell commands added, status changed from manual to automated (Ticket 22424)
28-Aug-24	3.0.0	UPDATE - All - MSOL and Azure AD cmdlet references updated to use Graph PowerShell (Ticket 17315)
2-Sep-24	3.0.0	UPDATE - Audit Policy is a Community Policy, Not GA - Removed potentially destructive community Audit Policy (Ticket 22321)
2-Sep-24	3.0.0	UPDATE - Azure Portal and Azure CLI audit procedures are inconsistent - Updated Description, Rationale, Audit, and Remediation to clarify intent (Ticket 22242)
3-Sep-24	3.0.0	UPDATE - Classic roles may be deprecated by 09-2024 - Remove reference to classic roles, only mention custom roles (Ticket 19474)
3-Sep-24	3.0.0	UPDATE - CLI command missing closing quotation marks - CLI command updated (Ticket 22286)
29-Aug-24	3.0.0	UPDATE - Conditional Access - All CA Recommendation profiles changed to "Level 2" (Ticket 22468)
28-Aug-24	3.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Assessment Status changed from Manual to Automated (Ticket 22438)
19-Aug-24	3.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Description, policy name, and parameter styling updated (Ticket 21900)

9-Aug-24	3.0.0	UPDATE - Ensure `User consent for applications` is set to `Do not allow user consent` - Updated MSOL commands to mggraph (Ticket 21705)
9-Aug-24	3.0.0	UPDATE - Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’ - Update msol powershell command to mggraph (Ticket 21704)
18-Aug-24	3.0.0	UPDATE - Ensure App Service Authentication is set up for apps in Azure App Service - Changes in CLI audit steps (Ticket 21096)
19-Aug-24	3.0.0	UPDATE - Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' Draft - Title and Prose updated from "Ensure FTP deployments are Disabled" (Ticket 22378)
19-Aug-24	3.0.0	UPDATE - Ensure 'HTTPS Only' is set to 'On' - Retitled and updated from "Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service" (Ticket 22376)
2-Sep-24	3.0.0	UPDATE - Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' - Marked as 'legacy', single server only (Ticket 22485)
9-Aug-24	3.0.0	UPDATE - Ensure Multi-factor Authentication is Required for Risky Sign-ins - Prose updated to reflect P2 licensing requirement (Ticket 22210)
27-Aug-24	3.0.0	UPDATE - Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) - Additional rationale context added (Ticket 22449)
19-Aug-24	3.0.0	UPDATE - Ensure only MFA enabled identities can access privileged Virtual Machine - Automation status changed to Manual (Ticket 21897)
2-Sep-24	3.0.0	UPDATE - Ensure Private Endpoints are used to access Storage Accounts - Consider making level 2 to consider requirement for DNS entries - Updated Impact to reflect cost, changed from Level 1 to Level 2 (Ticket 22279)
28-Aug-24	3.0.0	UPDATE - Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server - References updated for Flexible Server (Ticket 21891)
28-Aug-24	3.0.0	UPDATE - Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server - References updated for Flexible Server (Ticket 21892)
2-Sep-24	3.0.0	UPDATE - Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL flexible server - Marked as 'legacy', single server only (Ticket 22483)

2-Sep-24	3.0.0	UPDATE - Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server - Marked as 'legacy', single server only (Ticket 22484)
2-Sep-24	3.0.0	UPDATE - Ensure Soft Delete is Enabled for Azure Containers and Blob Storage - Update Audit/Remediate from CLI and Default Value for accuracy (Ticket 22280)
2-Sep-24	3.0.0	UPDATE - Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) - Update to Rationale explaining Manual Assessment Status (Ticket 22281)
29-Aug-24	3.0.0	UPDATE - Ensure that `Allow Blob Anonymous Access` is set to `Disabled` - Consider preview policy to replace the MODIFY policy being currently used. (Ticket 22282)
9-Aug-24	3.0.0	UPDATE - Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ - Assessment status changed to Automated (Ticket 21747)
9-Aug-24	3.0.0	UPDATE - Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ - Update msol powershell command to mggraph (Ticket 21746)
2-Sep-24	3.0.0	UPDATE - Ensure that an exclusionary Geographic Access Policy is considered - Updated Azure AD cmdlets to Graph PowerShell (Ticket 22459)
26-Aug-24	3.0.0	UPDATE - Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' - Added CLI & Powershell (Ticket 22413)
30-Aug-24	3.0.0	UPDATE - Ensure that 'Endpoint protection' component status is set to 'On' - Title changed, assessment status changed to Automated, prose updated for portal UI changes (Ticket 22417)
22-Jan-24	3.0.0	UPDATE - Ensure that Endpoint Protection for all Virtual Machines is installed - Newer policy ID added (Ticket 20579)
9-Aug-24	3.0.0	UPDATE - Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' - Assessment status changed to Automated (Ticket 22307)
9-Aug-24	3.0.0	UPDATE - Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' - Powershell audit and remediation procedures added (Ticket 21748)

9-Aug-24	3.0.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Assessment changed to Automated (Ticket 21749)
9-Aug-24	3.0.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Powershell updated to use mggraph (Ticket 21750)
23-Aug-24	3.0.0	UPDATE - Ensure that 'HTTP20enabled' is set to 'true' (if in use) - Prose updated to reflect 'app' or 'app services', not just 'web app' (Ticket 22273)
19-Aug-24	3.0.0	UPDATE - Ensure that 'HTTP20enabled' is set to 'true' (if in use) - Title and Prose updated to reflect the setting name more accurately (Ticket 22379)
19-Aug-24	3.0.0	UPDATE - Ensure that 'Java version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22182)
23-Aug-24	3.0.0	UPDATE - Ensure that 'Java version' is currently supported (if in use) - Prose updated to reflect 'app' or 'app services', not just 'web app' (Ticket 22272)
3-Aug-24	3.0.0	UPDATE - Ensure That Microsoft Defender for Containers Is Set To 'On' - Description updated to highlight Defender for Containers features (Ticket 20486)
30-Jan-24	3.0.0	UPDATE - Ensure That Microsoft Defender for Key Vault Is Set To 'On' - Fixed CLI typo (Ticket 19004)
30-Jan-24	3.0.0	UPDATE - Ensure That Microsoft Defender for Resource Manager Is Set To 'On' - Fixed CLI typo (Ticket 19006)
9-Aug-24	3.0.0	UPDATE - Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - Correct erroneous change to portal audit steps (Ticket 21073)
3-Sep-24	3.0.0	UPDATE - Ensure that Network Security Group Flow logs are captured and sent to Log Analytics - Clarity needed on Description and Audit Procedure - Recommendation updated for clarity (Ticket 17003)
19-Aug-24	3.0.0	UPDATE - Ensure that 'PHP version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22382)
19-Aug-24	3.0.0	UPDATE - Ensure that 'Python version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22381)

16-Aug-24	3.0.0	UPDATE - Ensure that 'Require Multi-Factor Authentication to register or join devices with Microsoft Entra ID' is set to 'Yes' - Added links to CA Policy and updated description and rationale (Ticket 22308)
9-Aug-24	3.0.0	UPDATE - Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes' - Assessment status changed to Automated (Ticket 21745)
15-Aug-24	3.0.0	UPDATE - Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) - Syntax correction & addition (Ticket 22060)
19-Aug-24	3.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults - Permission name corrected to 'List Secret' (Ticket 21899)
19-Aug-24	3.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults - Permission name corrected to 'List Secret' (Ticket 21898)
19-Aug-24	3.0.0	UPDATE - Ensure the Key Vault is Recoverable - Added Azure Policy (Ticket 21395)
3-Sep-24	3.0.0	UPDATE - Ensure Trusted Locations Are Defined - Updated Azure AD cmdlets to Graph PowerShell (Ticket 22458)
28-Aug-24	3.0.0	UPDATE - Ensure Trusted Locations Are Defined - Updated prose to alert of MFA requirement for Break-Glass Accounts (Ticket 22385)
29-Aug-24	3.0.0	UPDATE - Key Vault - Section moved into "Security" parent category section (Ticket 22470)
30-Aug-24	3.0.0	UPDATE - Multiple Methods of Audit and Remediation - Information article updated to address Microsoft Graph PowerShell (Ticket 22467)
2-Sep-24	3.0.0	UPDATE - Need to review variations between "Single Server" and "Flexible Server" - PostgreSQL recommendations updated to align with flexible server (Ticket 17688)
3-Sep-24	3.0.0	UPDATE - Please update Impact to consider new Microsoft best practice - Clarify that Conditional Access should be used instead if possible (Ticket 22141)
2-Sep-24	3.0.0	UPDATE - Propose updating the Assessment Status from Manual to Automated - Assessment Status changed from Manual to Automated (Ticket 22439)

2-Sep-24	3.0.0	UPDATE - Propose updating the Assessment Status from Manual to Automated - Assessment Status changed from Manual to Automated (Ticket 22442)
2-Sep-24	3.0.0	UPDATE - Proposing to update Assessment Status from Manual to Automated for "Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected" - Assessment Status changed from Manual to Automated (Ticket 22416)
2-Sep-24	3.0.0	UPDATE - Update Audit from Azure CLI steps, as 'application-insights' CLI extension is GA - Updated Audit CLI steps, command now GA (Ticket 22431)
2-Sep-24	3.0.0	UPDATE - Update Audit Procedure to include expected results - Updated audit from CLI command, added expected results for audit (Ticket 22440)
2-Sep-24	3.0.0	UPDATE - Update Audit Procedure to include expected results - Updated audit from CLI command, added expected results for audit (Ticket 22441)
28-Aug-24	3.0.0	UPDATE - Use Entra ID Client Authentication and Azure RBAC where possible - Policy added (Ticket 22320)
29-Dec-23	2.1.0	ADD - Ensure fewer than 5 users have global administrator assignment (Ticket 20550)
13-Feb-24	2.1.0	ADD - Ensure Multifactor Authentication is Required for Windows Azure Service Management API (Ticket 20670)
21-Dec-23	2.1.0	ADD - Ensure only MFA enabled identities can access privileged Virtual Machine (Ticket 19134)
13-Feb-24	2.1.0	ADD - Ensure that Microsoft Defender for External Attack Surface Monitoring is enabled (Ticket 20641)
16-Nov-23	2.1.0	ADD - Ensure that Private Endpoints are Used for Azure Key Vault - Virtual network service endpoints for Azure Key Vault (Ticket 15428)
13-Feb-24	2.1.0	ADD - Ensure Trusted Launch is enabled on Virtual Machines (Ticket 20534)
9-Jan-24	2.1.0	ADD - Method Header for Policy - "From Policy" header with applicable policy recommendations added to 100 recommendations (Ticket 15597)
13-Feb-24	2.1.0	DELETE - Ensure That Microsoft Defender for Databases Is Set To 'On' - Recommendation was duplicate to other defender recommendations (Ticket 18572)
27-Dec-23	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account -

		Vulnerability Assessment no longer need storage configuration (Ticket 17504)
27-Dec-23	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners' is set for each SQL Server - Now redundant with Microsoft defender for cloud settings (Ticket 19550)
13-Feb-24	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) setting 'Periodic recurring scans' is set to 'on' for each SQL server - Cannot change periodic scan settings on Defender for SQL (Ticket 19565)
27-Dec-23	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) setting 'Send scan reports to' is configured for a SQL server - Cannot change scan settings on Defender for SQL (Ticket 19567)
13-Feb-24	2.1.0	DELETE - Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible - Redundant recommendation (Ticket 18598)
2-Jan-24	2.1.0	DELETE - Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' - Remove and move to Compute Services BM (Ticket 19258)
22-Jan-24	2.1.0	DELETE - Ensure Access Review is Set Up for External Users in Microsoft Entra ID Privileged Identity Management - Duplicated intent of 1.5 (Ticket 20666)
21-Dec-23	2.1.0	UPDATE - Ensure that Network Watcher is 'Enabled' - changes to clarify (Ticket 19013)
25-Jan-24	2.1.0	UPDATE - Configuring Diagnostic Settings - Prose to include "Log Analytics" (Ticket 18595)
21-Dec-23	2.1.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Add CLI audit/remediation methods (Ticket 15959)
30-Jan-24	2.1.0	UPDATE - Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled - Updated Mitre mapping (Ticket 19963)
13-Feb-24	2.1.0	UPDATE - Ensure App Service Authentication is set up for apps in Azure App Service - Added/Updated CLI (Ticket 20539)

22-Dec-23	2.1.0	UPDATE - Ensure App Service Authentication is set up for apps in Azure App Service - Additional authentication-related recommendations added (Ticket 17197)
17-Jan-24	2.1.0	UPDATE - Ensure Multi-factor Authentication is Required for Risky Sign-ins - Added remediation step to require sign-in frequency every time (Ticket 20663)
16-Jan-24	2.1.0	UPDATE - Ensure Multifactor Authentication is Required to access Microsoft Admin Portals - Updated language and procedures for clarity and accuracy (Ticket 17689)
30-Jan-24	2.1.0	UPDATE - Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key - Mitre mapping added (Ticket 19415)
25-Jan-24	2.1.0	UPDATE - Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests - Portal procedures updated (Ticket 19116)
25-Jan-24	2.1.0	UPDATE - Ensure that a 'Diagnostic Setting' exists - Remediation updated to indicate option of 'partner solution' (Ticket 16249)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group - Audit procedure for portal updated (Ticket 19047)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18912)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Public IP Address rule - Audit procedure for portal updated (Ticket 19053)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Public IP Address rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18918)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - Audit procedure for portal updated (Ticket 19049)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18914)

25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule - Audit procedure for portal updated (Ticket 19051)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18916)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Audit procedure for portal updated (Ticket 19045)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Portal Remediation steps updated (Ticket 18910)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Removed '--location global' from Azure CLI remediation syntax (Ticket 18909)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Network Security Group - Audit procedure for portal updated (Ticket 19048)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Network Security Group - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18913)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Policy Assignment - Audit procedure for portal updated (Ticket 19046)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Policy Assignment - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18911)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Public IP Address rule - Audit procedure for portal updated (Ticket 19054)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Public IP Address rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18919)

25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Security Solution - Audit procedure for portal updated (Ticket 19050)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Security Solution - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18915)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule - Audit procedure for portal updated (Ticket 19052)
25-Jan-24	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18917)
13-Feb-24	2.1.0	UPDATE - Ensure That 'All users with the following roles' is set to 'Owner' - Updated CLI Syntax (Ticket 19204)
22-Jan-24	2.1.0	UPDATE - Ensure That 'All users with the following roles' is set to 'Owner' - Updated CLI syntax and CLI audit language for accuracy (Ticket 20643)
28-Dec-23	2.1.0	UPDATE - Ensure that an exclusionary Geographic Access Policy is considered - Remediation portal steps update (Ticket 16658)
30-Jan-24	2.1.0	UPDATE - Ensure that 'Auditing' is set to 'On' - Updated Mitre mapping (Ticket 19418)
25-Jan-24	2.1.0	UPDATE - Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' - CLI Syntax was updated for cleaner output (Ticket 19123)
13-Feb-24	2.1.0	UPDATE - Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On' - Procedures Updated (Ticket 17721)
30-Jan-24	2.1.0	UPDATE - Ensure that 'Enable key rotation reminders' is enabled for each Storage Account - Added audit and remediation procedures for powershell (Ticket 19490)
9-Jan-24	2.1.0	UPDATE - Ensure that Endpoint Protection for all Virtual Machines is installed - Updated Azure CLI query for easier review (Ticket 20551)

25-Jan-24	2.1.0	UPDATE - Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks - Audit procedure CLI updated (Ticket 18845)
26-Jan-24	2.1.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Default value corrected and prose updated with impact detail. (Ticket 19112)
21-Dec-23	2.1.0	UPDATE - Ensure that HTTP(S) access from the Internet is evaluated and restricted - include https in audit and remdiation (Ticket 19142)
30-Jan-24	2.1.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Rationale modified to explain that destination can be Storage Account or Log Analytics workspace (Ticket 19933)
30-Jan-24	2.1.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Updated CLI, removed retention period with deprecation timeline in additional information (Ticket 19129)
25-Jan-24	2.1.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Updates to Audit and Remediation Console steps (Ticket 18941)
30-Jan-24	2.1.0	UPDATE - Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' - Clarified description, rationale, and impact regarding "Disabled" policy effect (Ticket 19272)
30-Jan-24	2.1.0	UPDATE - Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' - CLI temporarily removed due to changes (Ticket 19124)
30-Jan-24	2.1.0	UPDATE - Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' - Title and policy initiative naming updated (Ticket 17557)
30-Jan-24	2.1.0	UPDATE - Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' - Updated Mitre mapping (Ticket 19416)
7-Dec-23	2.1.0	UPDATE - Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - wording updates to Audit and Remediation Azure Portal steps (Ticket 16656)

21-Dec-23	2.1.0	UPDATE - Ensure that Network Watcher is 'Enabled' - note locations where it wants network watcher to be enabled. (Ticket 17317)
30-Jan-24	2.1.0	UPDATE - Ensure That No Custom Subscription Administrator Roles Exist - Removed outdated assignable scope reference (Ticket 19115)
30-Jan-24	2.1.0	UPDATE - Ensure That No Custom Subscription Administrator Roles Exist - Updated Mitre mapping (Ticket 19417)
13-Feb-24	2.1.0	UPDATE - Ensure That 'PHP version' is the Latest, If Used to Run the Web App - CLI Updated (Ticket 16343)
25-Jan-24	2.1.0	UPDATE - Ensure That Private Endpoints Are Used Where Possible - Automation status change from Manual to Automated (Ticket 17324)
11-Jan-24	2.1.0	UPDATE - Ensure that 'Public access level' is disabled for storage accounts with blob containers - Added Language for Classic Deployment Model for Storage Accounts (Ticket 20305)
9-Jan-24	2.1.0	UPDATE - Ensure that RDP access from the Internet is evaluated and restricted - Blocking source 0.0.0.0 is now included. (Ticket 16169)
30-Jan-24	2.1.0	UPDATE - Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) - Automation Status changed from 'Automated' to 'Manual' (Ticket 18775)
25-May-23	2.1.0	UPDATE - Ensure that 'Users can create Azure AD Tenants' is set to 'No' - Added Powershell & Changed to Manual Temporarily (Ticket 18493)
14-Dec-23	2.1.0	UPDATE - Ensure that 'Users can create Azure AD Tenants' is set to 'No' - Wording change to tile and audit steps (Ticket 18690)
9-Jan-24	2.1.0	UPDATE - Ensure the Key Vault is Recoverable - Updated language to indicate soft delete option is deprecated (Ticket 18964)
25-Jan-24	2.1.0	UPDATE - Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible - Updated portal/Az CLI/PowerShell Audit Procedures/Remediation Procedures (Ticket 17266)

25-Jan-24	2.1.0	UPDATE - Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server - Included consideration for TLS 1.3 (Ticket 17731)
21-Dec-23	2.1.0	UPDATE - Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service - change in portal steps for audit and remediation procedure (Ticket 17757)
22-Jan-24	2.1.0	UPDATE - Microsoft Defender for Cloud - All MDC recommendations with Policy updated to 'Automated' (Ticket 18241)
25-Jan-24	2.1.0	UPDATE - Rename "Azure Active Directory" to "Microsoft Entra ID" everywhere in the document (Ticket 19273)