

CIS Microsoft Azure Compute Services Benchmark

v2.0.0 - 06-27-2025

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

Terms of Use	1
Table of Contents	2
Overview	7
Important Usage Information.....	7
Key Stakeholders.....	7
Apply the Correct Version of a Benchmark	8
Exceptions	8
Remediation	9
Summary.....	9
Target Technology Details.....	10
Intended Audience	10
Consensus Guidance	11
Typographical Conventions	12
Recommendation Definitions.....	13
Title	13
Assessment Status	13
Automated	13
Manual.....	13
Profile	13
Description	13
Rationale Statement	13
Impact Statement.....	14
Audit Procedure.....	14
Remediation Procedure	14
Default Value	14
References	14
CIS Critical Security Controls® (CIS Controls®).....	14
Additional Information	14
Profile Definitions	15
Acknowledgements.....	16
Recommendations	17
1 Introduction.....	17
1.1 CIS Microsoft Azure Foundations Benchmarks	18
1.2 CIS Microsoft Azure Service Category Benchmarks	19
1.3 Multiple Methods of Audit and Remediation.....	20
2 App Service.....	23

Resources for App Service	23
2.1 App Service Apps	24
2.1.1 Ensure 'Java version' is currently supported (if in use) (Manual)	25
2.1.2 Ensure 'Python version' is currently supported (if in use) (Manual)	29
2.1.3 Ensure 'PHP version' is currently supported (if in use) (Manual)	32
2.1.4 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)	35
2.1.5 Ensure 'FTP State' is set to 'FTPS only' or 'Disabled' (Automated)	39
2.1.6 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	42
2.1.7 Ensure 'HTTPS Only' is set to 'On' (Automated)	45
2.1.8 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	48
2.1.9 Ensure end-to-end TLS encryption is enabled (Automated)	51
2.1.10 Ensure 'Remote debugging' is set to 'Off' (Automated)	54
2.1.11 Ensure incoming client certificates are enabled and required (if in use) (Automated) ..	57
2.1.12 Ensure 'App Service authentication' is set to 'Enabled' (Automated)	60
2.1.13 Ensure managed identities are configured (Automated)	63
2.1.14 Ensure public network access is disabled (Automated)	66
2.1.15 Ensure App Service plan SKU supports private endpoints (Automated)	69
2.1.16 Ensure private endpoints are used to access App Service apps (Automated)	73
2.1.17 Ensure private endpoints used to access App Service apps use private DNS zones (Manual)	76
2.1.18 Ensure app is integrated with a virtual network (Automated)	78
2.1.19 Ensure configuration is routed through the virtual network integration (Automated)	82
2.1.20 Ensure all traffic is routed through the virtual network (Automated)	84
2.1.21 Ensure cross-origin resource sharing does not allow all origins (Automated)	87
2.2 App Service Deployment Slots	90
2.2.1 Ensure 'Java version' is currently supported (if in use) (Manual)	91
2.2.2 Ensure 'Python version' is currently supported (if in use) (Manual)	94
2.2.3 Ensure 'PHP version' is currently supported (if in use) (Manual)	97
2.2.4 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)	100
2.2.5 Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)	104
2.2.6 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	107
2.2.7 Ensure 'HTTPS Only' is set to 'On' (Automated)	110
2.2.8 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	113
2.2.9 Ensure end-to-end TLS encryption is enabled (Automated)	116
2.2.10 Ensure 'Remote debugging' is set to 'Off' (Automated)	119
2.2.11 Ensure incoming client certificates are enabled and required (if in use) (Automated) ..	122
2.2.12 Ensure managed identities are configured (Automated)	125
2.2.13 Ensure public network access is disabled (Automated)	128
2.2.14 Ensure deployment slot is integrated with a virtual network (Automated)	131
2.2.15 Ensure configuration is routed through the virtual network integration (Automated) ..	134
2.2.16 Ensure all traffic is routed through the virtual network (Automated)	136
2.2.17 Ensure cross-origin resource sharing does not allow all origins (Automated)	139
2.3 Function Apps	142
2.3.1 Ensure 'Java version' is currently supported (if in use) (Manual)	143
2.3.2 Ensure 'Python version' is currently supported (if in use) (Manual)	146
2.3.3 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)	149
2.3.4 Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)	152
2.3.5 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	155
2.3.6 Ensure 'HTTPS Only' is set to 'On' (Automated)	158
2.3.7 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	161
2.3.8 Ensure end-to-end TLS encryption is enabled (Automated)	164
2.3.9 Ensure 'Remote debugging' is set to 'Off' (Automated)	166
2.3.10 Ensure incoming client certificates are enabled and required (if in use) (Automated) ..	169
2.3.11 Ensure 'App Service authentication' is set to 'Enabled' (Automated)	172
2.3.12 Ensure managed identities are configured (Automated)	175
2.3.13 Ensure public network access is disabled (Automated)	178

2.3.14 Ensure function app is integrated with a virtual network (Automated)	181
2.3.15 Ensure configuration is routed through the virtual network integration (Automated) ..	184
2.3.16 Ensure all traffic is routed through the virtual network (Automated).....	186
2.3.17 Ensure cross-origin resource sharing does not allow all origins (Automated)	189
2.4 Functions Deployment Slots	192
2.4.1 Ensure 'Java version' is currently supported (if in use) (Manual)	193
2.4.2 Ensure 'Python version' is currently supported (if in use) (Manual)	196
2.4.3 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated).....	199
2.4.4 Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated).....	202
2.4.5 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	205
2.4.6 Ensure 'HTTPS Only' is set to 'On' (Automated)	208
2.4.7 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	211
2.4.8 Ensure end-to-end TLS encryption is enabled (Automated)	214
2.4.9 Ensure 'Remote debugging' is set to 'Off' (Automated)	216
2.4.10 Ensure incoming client certificates are enabled and required (if in use) (Automated)	219
2.4.11 Ensure managed identities are configured (Automated)	222
2.4.12 Ensure public network access is disabled (Automated)	225
2.4.13 Ensure deployment slot is integrated with a virtual network (Automated).....	228
2.4.14 Ensure configuration is routed through the virtual network integration (Automated) ..	230
2.4.15 Ensure all traffic is routed through the virtual network (Automated).....	232
2.4.16 Ensure cross-origin resource sharing does not allow all origins (Automated)	235
2.5 Ensure Azure Key Vaults are Used to Store Secrets (Manual).....	238
2.6 Ensure App Service Environment is deployed with an internal load balancer (Automated)	243
2.7 Ensure App Service Environment is provisioned with v3 or higher (Automated)	245
2.8 Ensure App Service Environment has internal encryption enabled (Automated)	247
2.9 Ensure App Service Environment has TLS 1.0 and 1.1 disabled (Automated).....	250
2.10 Ensure App Service Environment has TLS cipher suite ordering configured (Automated)	252
3 Azure Container Instances	255
Resources for Azure Container Instances	255
3.1 Ensure Private Virtual Networks are used for Container Instances (Manual)	256
3.2 Ensure a Managed Identity is used for interactions with other Azure services (Manual).	258
3.3 Ensure the principle of least privilege is used when assigning roles to a Managed Identity	261
4 Azure CycleCloud.....	264
Resources for Azure CycleCloud	264
4.1 Ensure SSL is configured for CycleCloud (Manual)	265
5 Azure Dedicated Host	267
Resources for Azure Dedicated Host.....	267
6 Azure Functions (Reference).....	268
Resources for Azure Functions.....	268
7 Azure Kubernetes Service (Reference)	269
Resources for Azure Kubernetes Service	269
8 Azure Quantum	270
Resources for Azure Quantum.....	270
9 Azure Service Fabric	271
Resources for Azure Service Fabric	271
10 Azure Spot Virtual Machines (Reference)	272
Resources for Azure Spot Virtual Machines	272

11 Azure Spring Apps (Retiring)	273
Resources for Azure Spring Apps	273
12 Azure Virtual Desktop (Reference)	274
Resources for Azure Virtual Desktop	274
13 Azure VM Image Builder	275
Resources for Azure VM Image Builder	275
14 Azure VMware Solution	276
Resources for Azure VMware Solution	276
15 Batch	277
Resources for Batch	277
15.1 Ensure Batch account is set to use customer-managed keys to encrypt data (Manual)	278
15.2 Ensure Batch pools disk encryption is set enabled (Automated)	281
15.3 Ensure local authentication methods for accounts are disabled (Automated)	285
15.4 Ensure Private endpoints are considered for Batch accounts (Automated)	288
15.5 Ensure public network access is disabled for Batch accounts (Automated)	291
15.6 Ensure private DNS zones for private endpoints that connect to Batch accounts are configured. (Manual)	294
15.7 Ensure Diagnostics settings logs for Batch accounts are enabled (Automated)	298
16 Linux Virtual Machines (Reference)	302
Resources for Linux Virtual Machines	302
17 SQL Server on Azure Virtual Machines (Reference)	303
Resources for SQL Server on Azure Virtual Machines	303
18 Static Web Apps (Reference)	304
Resources for Static Web Apps	304
19 Virtual Machine Scale Sets	305
Resources for Virtual Machine Scale Sets	305
20 Virtual Machines	306
Resources for Virtual Machines	306
20.1 Ensure Virtual Machines are utilizing Managed Disks (Automated)	307
20.2 Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)	310
20.3 Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)	313
20.4 Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Automated)	316
20.5 Ensure that 'Enable Data Access Authentication Mode' is 'Checked' (Automated)	320
20.6 Ensure that Only Approved Extensions Are Installed (Manual)	323
20.7 Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)	326
20.8 [Legacy] Ensure that VHDs are Encrypted (Manual)	328
20.9 Ensure only MFA enabled identities can access privileged Virtual Machine (Manual)	331
20.10 Ensure Trusted Launch is enabled on Virtual Machines (Automated)	334
20.11 Ensure that encryption at host is enabled (Automated)	338
Appendix: Summary Table	342
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	350
Appendix: CIS Controls v7 IG 2 Mapped Recommendations	352
Appendix: CIS Controls v7 IG 3 Mapped Recommendations	356
Appendix: CIS Controls v7 Unmapped Recommendations	361

<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations</i>	<i>362</i>
<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations</i>	<i>364</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations</i>	<i>369</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>374</i>
<i>Appendix: Change History</i>	<i>375</i>

Overview

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

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

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

Important Usage Information

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

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

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

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

Key Stakeholders

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

Apply the Correct Version of a Benchmark

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

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

Exceptions

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

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

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

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

Remediation

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

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

The following is a reasonable remediation approach to follow:

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

Summary

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

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

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

Target Technology Details

This benchmark - CIS Microsoft Azure Compute Services Benchmark - will provide secure configuration recommendations for Azure products that Microsoft has categorized as “Compute” services.

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

- 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
- Linux Virtual Machines
- SQL Server on Azure Virtual Machines
- Static Web Apps
- Virtual Machine Scale Sets
- Virtual Machines

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

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

Intended Audience

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

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

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

- **Level 2**

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

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

Acknowledgements

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

Contributor

Sagar Chhatrala
Steve Johnson
Miles Nukwu
Mark Weaver
Rogier Carper
Robert Burton
Michael Born

Editor

Rachel Rice
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://learn.microsoft.com/en-us/cli/azure/install-azure-cli>

For PowerShell, the following cmdlets are required:

1. Azure PowerShell: <https://learn.microsoft.com/en-us/powershell/azure/install-azure-powershell?view=azps-13.4.0>
2. Microsoft Graph PowerShell: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/installation?view=graph-powershell-1.0>

Authenticating with Azure CLI

Run the following command from either PowerShell or command prompt:

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

Authenticating with PowerShell

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

```
Connect-AzAccount
```

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>

- AzPolicyAdvertiser - 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 App Service

This section covers security best practice recommendations for App Service.

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

The CIS Microsoft Azure Community is here:

<https://workbench.cisecurity.org/communities/72>.

Resources for App Service

Azure Product Page:

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

App Service service overview:

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

Microsoft Cloud Security Baseline for App Service:

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

2.1 App Service Apps

2.1.1 Ensure 'Java version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Java may be deprecated and no longer supported. Using a supported version of Java for App Service apps is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of currently supported versions of Java here:

<https://www.oracle.com/java/technologies/java-se-support-roadmap.html>

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, ensure that for a **Stack** of **Java**, the **Major Version** and **Minor Version** reflect a currently supported release, and that the **Java web server version** is set to the **auto-update** option.
5. Repeat steps 1-4 for each app.

NOTE: No action is required if **Java version** is set to **Off**, as Java is not used by your app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to check the Java version:

```
az webapp config show --resource-group <resource-group-name> --name <app-name> --query "{LinuxFxVersion:linuxFxVersion, WindowsFxVersion:windowsFxVersion, JavaVersion:javaVersion, JavaContainerVersion:javaContainerVersion, JavaContainer:javaContainer}"
```

If Java is in use, ensure the version is currently supported.

Audit from PowerShell

For each application, store the application information within an object, and then interrogate the **SiteConfig** information for that application object:

```
$app = Get-AzWebApp -Name <app-name> -ResourceGroup <resource-group-name>

$app.SiteConfig |Select-Object LinuxFxVersion, WindowsFxVersion, JavaVersion,
JavaContainerVersion, JavaContainer
```

If Java is in use, ensure the version is currently supported.

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:** [496223c3-ad65-4ecd-878a-bae78737e9ed](#) - **Name:** 'App Service apps that use Java should use a specified 'Java version''

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **App Services**
3. Click on each App
4. Under **Settings** section, click on **Configuration**
5. Click on the **General settings** pane and ensure that for a **Stack of Java** the **Major Version** and **Minor Version** reflect a currently supported release, and that the **Java web server version** is set to the **auto-update** option.

NOTE: No action is required if **Java version** is set to **Off**, as Java is not used by your app.

Remediate from Azure CLI

To see the list of supported runtimes:

```
az webapp list-runtimes
```

To set a currently supported Java version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
[--java-version <JAVA_VERSION> --java-container <JAVA_CONTAINER> --java-
container-version <JAVA_CONTAINER_VERSION> [--windows-fx-version
<JAVA_RUNTIME_VERSION>] [--linux-fx-version <JAVA_RUNTIME_VERSION>]
```

If creating a new application to use a currently supported version of Java, run the following commands.

To create an app service plan:

```
az appservice plan create --resource-group <RESOURCE_GROUP_NAME> --name
<PLAN_NAME> --location <LOCATION> [--is-linux --number-of-workers <INT> --sku
<PRICING_TIER>] [--hyper-v --sku <PRICING_TIER>]
```

Get the app service plan ID:

```
az appservice plan list --query "[].{Name:name, ID:id, SKU:sku,
Location:location}"
```

To create a new Java web application using the retrieved app service ID:

```
az webapp create --resource-group <RESOURCE_GROUP_NAME> --plan
<APP_SERVICE_PLAN_ID> --name <app name> [--linux-fx-version
<JAVA_RUNTIME_VERSION>] [--windows-fx-version <JAVA_RUNTIME_VERSION>]
```

Remediate from PowerShell

As of this writing, there is no way to update an existing application's **SiteConfig** or set a new application's **SiteConfig** settings during creation via PowerShell.







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-language-java-deploy-run>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://www.oracle.com/java/technologies/java-se-support-roadmap.html>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.1.2 Ensure 'Python version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Python may be deprecated and no longer supported. Using a supported version of Python for App Service apps is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions (given a status of "security") of Python here: <https://devguide.python.org/versions/>

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, ensure that for a **Stack** of **Python**, the **Major version** and **Minor version** reflect a currently supported release.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the Python version:

```
az webapp config show --resource-group <resource-group-name> --name <app-name> --query  
"{LinuxFxVersion:linuxFxVersion,WindowsFxVersion:windowsFxVersion,PythonVersion:pythonVersion}"
```

If Python is in use, ensure the version is currently supported.

Audit from PowerShell

```
$app = Get-AzWebApp -Name <app-name> -ResourceGroup <resource-group-name>  
$app.SiteConfig |Select-Object LinuxFXVersion, WindowsFxVersion,  
PythonVersion
```

If Python is in use, ensure the version is currently supported.

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:** [7008174a-fd10-4ef0-817e-fc820a951d73](#) - **Name:** 'App Service apps that use Python should use a specified 'Python version''

Remediation:

Note: No action is required if Python is not in use.

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, for a **Stack** of **Python**, set the **Major version** and **Minor version** to a currently supported release.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each app requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az webapp list-runtimes
```

For each app requiring remediation, run the following command with the appropriate parameters to update the Python version:

```
az webapp config set --resource-group <resource-group-name> --name <app-name>
[--windows-fx-version "PYTHON|<version>"] [--linux-fx-version
"PYTHON|<version>"]
```







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#configure-language-stack-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://devguide.python.org/versions/>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp>
6. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.1.3 Ensure 'PHP version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of PHP may be deprecated and no longer supported. Using a supported version of PHP for App Service apps is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions of PHP here:

<https://www.php.net/supported-versions.php>

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, ensure that for a **Stack** of **PHP**, the **Major version** and **Minor version** reflect a currently supported release.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the PHP version:

```
az webapp config show --resource-group <resource-group-name> --name <app-name> --query "{LinuxFxVersion:linuxFxVersion,PhpVersion:phpVersion}"
```

If PHP is in use, ensure the version is currently supported.

Audit from PowerShell

Run the following command to list apps:

```
Get-AzWebApp
```

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

```
$app = Get-AzWebApp -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the PHP version:

```
$app.SiteConfig | select-object LinuxFXVersion, PhpVersion
```

If PHP is in use, ensure the version is currently supported.
Repeat for each app.

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:** [7261b898-8a84-4db8-9e04-18527132abb3](#) - **Name:** 'App Service apps that use PHP should use a specified 'PHP version''

Remediation:

Note: No action is required if PHP is not in use.

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, for a **Stack of PHP**, set the **Major version** and **Minor version** to a currently supported release.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each app requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az webapp list-runtimes
```

For each app requiring remediation, run the following command with the appropriate parameters to update the PHP version:

```
az webapp config set --resource-group <resource-group-name> --name <app-name> [--linux-fx-version <php-runtime-version>][--php-version <php-version>]
```

Remediate from PowerShell

For each app requiring remediation, run the following command to update the PHP version:

```
Set-AzWebApp -ResourceGroupName <resource-group-name> -Name <app-name> -phpVersion <php-version>
```

Note: Currently, there is no way to update an app's **Linux FX Version** setting using PowerShell.







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#general-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://www.php.net/supported-versions.php>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp>
6. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
7. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp>

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.			

2.1.4 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

Basic Authentication Publishing Credentials provides the ability to publish—or deploy to—an App Service app without a centralized Identity Provider. For a more effective, capable, and secure solution for Identity, Authentication, Authorization, and Accountability, a centralized Identity Provider such as Entra ID is strongly advised.

Rationale:

Basic Authentication introduces an identity silo for privileged access to a resource and produces logging which may not provide a full chain of accountability. This can be exploited in numerous ways and represents a significant vulnerability and attack vector.

Impact:

Disabling 'Basic Auth Publishing Credentials' will prevent the following deployment methods from working:

FTP Basic Auth Publishing Credentials:

- FTP
- FTPS

SCM Basic Auth Publishing Credentials:

- Local Git
- GitHub
- Azure Repos
- Bitbucket
- Visual Studio (Version 17.12 and earlier)

If this recommendation cannot be implemented because one of the above listed deployment methods is necessary and cannot be adapted, compensating controls (e.g. using FTPS Only and disabling only "SCM Basic Auth Publishing Credentials") are recommended to reduce potential attack surface.

An Identity Provider that can be used by the App Service app for authenticating users is required.

Audit:

Audit from Azure Portal

1. Search for, and open **App Services** from the search bar.
2. For each App Service listed:
3. Click on the App Service name.
4. Under the **Settings** menu item, click on **Configuration**
5. Under the **General settings** tab, scroll down to locate the two Basic Auth settings:
 - **SCM Basic Auth Publishing Credentials**
 - **FTP Basic Auth Publishing Credentials**

Both radio buttons should indicate a status of **Off**.
Repeat this procedure for each App Service.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the basic authentication for FTP setting:

```
az resource show --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name> --query properties.allow
```

Ensure that **false** is returned.

For each app, run the following command to get the basic authentication for SCM setting:

```
az resource show --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name> --query properties.allow
```

Ensure that **false** is returned.

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:** [871b205b-57cf-4e1e-a234-492616998bf7](#) - **Name:** 'App Service apps should have local authentication methods disabled for FTP deployments'
- **Policy ID:** [aede300b-d67f-480a-ae26-4b3dfb1a1fdc](#) - **Name:** 'App Service apps should have local authentication methods disabled for SCM site deployments'

Remediation:

Remediate from Azure Portal

1. Search for, and open **App Services** from the search bar.
2. For each App Service listed:
3. Click on the App Service name.
4. Under the **Settings** menu item, click on **Configuration**
5. Under the **General settings** tab, scroll down to locate the two Basic Auth settings:
 - Set the **SCM Basic Auth Publishing Credentials** radio button to **Off**
 - Set the **FTP Basic Auth Publishing Credentials** radio button to **Off**

CAUTION: The new settings are not yet applied. Applying them may cause your App Service resource to restart - proceed with caution. Click the **Save** button, then click **Continue** to apply the updated configuration. Repeat this procedure for each App Service.

Remediate from Azure CLI

For each app requiring remediation, run the following command to disable basic authentication for FTP:

```
az resource update --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name> --set properties.allow=false
```

For each app requiring remediation, run the following command to disable basic authentication for SCM:

```
az resource update --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name> --set properties.allow=false
```





Default Value:

Basic authentication is disabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-basic-auth-disable>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.1.5 Ensure 'FTP State' is set to 'FTPS only' or 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

By default, App Service supports deployment over FTP. If FTP is essential for a deployment workflow, FTPS should be enforced for all App Service apps.

If FTPS is not explicitly required, the recommended setting is **Disabled**.

Rationale:

FTP is an unencrypted network protocol that transmits data—including passwords—in clear text. The use of this protocol can lead to both data and credential compromise and can present opportunities for exfiltration, persistence, and lateral movement.

Impact:

Deployment workflows that rely on FTP or FTPS rather than WebDeploy or HTTPS endpoints may be affected.

Audit:

Audit from Azure Portal

1. Go to the Azure Portal
2. Select **App Services**
3. Click on an app
4. Select **Settings** and then **Configuration**
5. Under **General Settings**, for the **Platform Settings**, the **FTP state** should not be set to **All allowed**

Audit from Azure CLI

List webapps to obtain the ids.

```
az webapp list
```

List the publish profiles to obtain the username, password, and ftp server url.

```
az webapp deployment list-publishing-profiles --ids <ids>
{
  "publishUrl": <URL_FOR_WEB_APP>,
  "userName": <USER_NAME>,
  "userPWD": <USER_PASSWORD>,
}
```


Audit from PowerShell

List all Web Apps:

```
Get-AzWebApp
```

For each app:

```
Get-AzWebApp -ResourceGroupName <resource group name> -Name <app name> |  
Select-Object -ExpandProperty SiteConfig
```

In the output, look for the value of **FtpsState**. If its value is **AllAllowed** the setting is out of compliance. Any other value is considered 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:** [4d24b6d4-5e53-4a4f-a7f4-618fa573ee4b](#) - **Name:** 'App Service apps should require FTPS only'

Remediation:

Remediate from Azure Portal

1. Go to the Azure Portal
2. Select **App Services**
3. Click on an app
4. Select **Settings** and then **Configuration**
5. Under **General Settings**, for the **Platform Settings**, the **FTP state** should be set to **Disabled** or **FTPS Only**

Remediate from Azure CLI

For each out of compliance application, run the following choosing either 'disabled' or 'FtpsOnly' as appropriate:

```
az webapp config set --resource-group <resource group name> --name <app name>  
--ftps-state [disabled|FtpsOnly]
```

Remediate from PowerShell

For each out of compliance application, run the following:

```
Set-AzWebApp -ResourceGroupName <resource group name> -Name <app name> -  
FtpsState <Disabled or FtpsOnly>
```







Default Value:

By default, FTP state is set to **FTPS only**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/deploy-ftp>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-security>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit>
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
5. <https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/create-or-update-configuration#ftpsstate>
6. <https://learn.microsoft.com/en-us/cli/azure/webapp>
7. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
8. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

2.1.6 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for HTTP, either due to security flaws or to include additional functionalities. Using the latest HTTP version allows apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.

Rationale:

Newer versions may contain security enhancements and additional functionalities. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

HTTP 2.0 has additional performance improvements for the head-of-line blocking problem of the old HTTP version, header compression, and request prioritization. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient mechanisms for data streaming.

Impact:

Most modern browsers support the HTTP/2 protocol over TLS only, while non-encrypted traffic continues to use HTTP/1.1. To ensure that client browsers connect to your app with HTTP/2, either purchase an App Service Certificate for your app's custom domain or bind a third-party certificate.

NOTE: HTTP/2 cannot be used in tandem with mutual authentication or client certificates.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, ensure that **HTTP version** is set to **2.0**.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the **http20Enabled** setting:

```
az webapp config show --resource-group <resource-group-name> --name <app-name> --query http20Enabled
```

Ensure that **true** is returned.

Audit from PowerShell

Run the following command to list apps:

```
Get-AzWebApp
```

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

```
$app = Get-AzWebApp -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the **Http20Enabled** setting:

```
$app.SiteConfig.Http20Enabled
```

Ensure that **True** is returned.

Repeat for each app.

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:** [8c122334-9d20-4eb8-89ea-ac9a705b74ae](#) - **Name:** 'App Service apps should use latest 'HTTP Version''

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, set **HTTP version** to **2.0**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each app requiring remediation.

Remediate from Azure CLI

For each app requiring remediation, run the following command to enable

http20Enabled:

```
az webapp config set --resource-group <resource-group-name> --name <app-name>
--http20-enabled true
```







Default Value:

By default, **HTTP version** is set to **1.1**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#general-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://learn.microsoft.com/en-us/cli/azure/webapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>

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.			

2.1.7 Ensure 'HTTPS Only' is set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

Azure App Service allows apps to run under both HTTP and HTTPS by default. Apps can be accessed by anyone using non-secure HTTP links by default. Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic.

Rationale:

Enabling HTTPS-only traffic will redirect all non-secure HTTP requests to HTTPS ports. HTTPS uses the TLS/SSL protocol to provide a secure connection which is both encrypted and authenticated. It is therefore important to support HTTPS for the security benefits.

Impact:

When it is enabled, every incoming HTTP request is redirected to the HTTPS port. This means an extra level of security will be added to the HTTP requests made to the app.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **App Services**
3. For each App Service
4. Under **Setting** section, click on **Configuration**
5. Under the **General Settings** tab, ensure that **HTTPS Only** is set to **On** under **Platform Settings**

Audit from Azure CLI

To check HTTPS-only traffic value for an existing app, run the following command,

```
az webapp show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query httpsOnly
```

The output should return **true** if HTTPS-only traffic value is set to **On**.

Audit from PowerShell

List all the web apps configured within the subscription.

```
Get-AzWebApp | Select-Object ResourceGroup, Name, HttpsOnly
```

For each web app review the **HttpsOnly** setting and make sure it 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:** [a4af4a39-4135-47fb-b175-47fbdf85311d](#) - **Name:** 'App Service apps should only be accessible over HTTPS'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **App Services**
3. For each App Service
4. Under **Setting** section, click on **Configuration**
5. Under the **General Settings** tab, set **HTTPS Only** to **On** under **Platform Settings**

Remediate from Azure CLI

To set HTTPS-only traffic value for an existing app, run the following command:

```
az webapp update --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --set httpsOnly=true
```

Remediate from PowerShell

```
Set-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> -HttpsOnly $true
```





Default Value:

HTTPS Only is disabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-security#https-and-certificates>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://techcommunity.microsoft.com/t5/azure-paas-blog/enable-https-setting-on-azure-app-service-using-azure-policy/ba-p/3286603>
4. <https://learn.microsoft.com/en-us/cli/azure/webapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
6. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp>

CIS Controls:

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

2.1.8 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)

Profile Applicability:

- Level 1

Description:

The TLS (Transport Layer Security) protocol secures the transmission of data over the internet using standard encryption technology. App Service apps use TLS 1.2 for the **Minimum Inbound TLS Version** by default and allow for the use of TLS versions 1.0, 1.1, and 1.3. NIST strongly suggests the use of TLS 1.2 and recommends the adoption of TLS 1.3.

Rationale:

TLS 1.0 and 1.1 are outdated and vulnerable to security risks. Since TLS 1.2 and TLS 1.3 provide enhanced security and improved performance, it is highly recommended to use TLS 1.2 or higher whenever possible.

Impact:

Using the latest TLS version may affect compatibility with clients and backend services.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, ensure that **Minimum Inbound TLS Version** is set to **1.2** or higher.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the TLS version setting:

```
az webapp config show --resource-group <resource-group-name> --name <app-name> --query minTlsVersion
```

Ensure that **"1.2"** or higher is returned.

Audit from PowerShell

Run the following command to list apps:

```
Get-AzWebApp
```

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

```
$app = Get-AzWebApp -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the TLS version setting:

```
$app.SiteConfig.MinTlsVersion
```

Ensure that the command returns **1.2** or higher.

Repeat for each app.

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:** [f0e6e85b-9b9f-4a4b-b67b-f730d42f1b0b](#) - **Name:** 'App Service apps should use the latest TLS version'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, click the drop-down next to **Minimum Inbound TLS Version** and select **1.2** or higher.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each app requiring remediation.

Remediate from Azure CLI

For each app requiring remediation, run the following command to update the TLS version:

```
az webapp config set --resource-group <resource-group-name> --name <app-name> --min-tls-version <1.2|1.3>
```

Remediate from PowerShell

For each app requiring remediation, run the following command to update the TLS version:

```
Set-AzWebApp -ResourceGroupName <resource-group-name> -Name <app-name> -MinTlsVersion <1.2|1.3>
```





Default Value:

By default, TLS version is set to 1.2.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-bindings#how-can-i-change-the-minimum-tls-versions-for-the-app>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-8-detect-and-disable-insecure-services-and-protocols>
4. <https://learn.microsoft.com/en-us/cli/azure/webapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
6. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp>
7. <https://csrc.nist.gov/news/2019/nist-publishes-sp-800-52-revision-2>

CIS Controls:

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

2.1.9 Ensure end-to-end TLS encryption is enabled (Automated)

Profile Applicability:

- Level 1

Description:

End-to-end (E2E) TLS encryption ensures that front-end to worker communication within App Service apps is encrypted using TLS. Without this feature, while incoming HTTPS requests are encrypted to the front ends, the traffic from front ends to workers running the application workloads would travel unencrypted inside Azure's infrastructure.

Rationale:

E2E TLS helps ensure full encryption of traffic between:

- Clients and front ends
- Front ends and worker processes hosting the application

Impact:

Enabling end-to-end TLS encryption may introduce minimal latency and require additional configuration of certificates and HTTPS settings to ensure compatibility.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, ensure that **Enable end-to-end TLS encryption** is set to **On**.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the end-to-end TLS encryption setting:

```
az webapp show --resource-group <resource-group-name> --name <app-name> --query endToEndEncryptionEnabled
```

Ensure that the command returns **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:** [af1d7e88-c1c8-4ea8-be1f-87bff0df9101](#) - **Name:** 'App Service apps should enable end to end encryption'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, next to **Enable end-to-end TLS encryption**, click the radio button next to **On**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each app requiring remediation.

Remediate from Azure CLI

For each app requiring remediation, run the following command to enable end-to-end TLS encryption:

```
az resource update --resource-group <resource-group-name> --name <app-name> --resource-type "Microsoft.Web/sites" --set properties.endToEndEncryptionEnabled=true
```





Default Value:

By default, end-to-end TLS encryption is disabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-tls#end-to-end-tls-encryption>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.1.10 Ensure 'Remote debugging' is set to 'Off' (Automated)

Profile Applicability:

- Level 1

Description:

Remote debugging allows an App Service app to be debugged in real-time directly in the Azure environment. When remote debugging is enabled, it opens a communication channel that could potentially be exploited by unauthorized users if not properly secured.

Rationale:

Disabling remote debugging on an App Service app is primarily about enhancing security.

Remote debugging opens a communication channel that can be exploited by attackers. By disabling it, you reduce the number of potential entry points for unauthorized access.

If remote debugging is enabled without proper access controls, it can allow unauthorized users to connect to your application, potentially leading to data breaches or malicious code execution.

During a remote debugging session, sensitive information might be exposed. Disabling remote debugging helps ensure that such data remains secure. This minimizes the use of remote access tools to reduce risk.

Impact:

You will not be able to connect to your application from a remote location to diagnose and fix issues in real-time. You will not be able to step through code, set breakpoints, or inspect variables and the call stack while the application is running on the server. Remote debugging is particularly useful for diagnosing issues that only occur in the production environment. Without it, you will need to rely on logs and other diagnostic tools.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **App Services**
3. Click on each App
4. Under **Setting** section, Click on **Configuration**
5. Under the **General settings** tab, check the **Remote debugging** option. Ensure it is set to **Off**.

Audit from Azure CLI

To check remote debugging status for an existing app, run the following command,

```
az webapp config show --resource-group <resource_group_name> --name  
<app_name> --query remoteDebuggingEnabled
```

The output should be **false** if remote debugging is disabled.

Audit from PowerShell

To check remote debugging status for an existing app, run the following command,

```
Get-AzWebApp -ResourceGroupName <resource_group_name> -Name <app_name>  
|Select-Object -ExpandProperty SiteConfig
```

The output of **remoteDebuggingEnabled** should be **false** if remote debugging is 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:** [cb510bfd-1cba-4d9f-a230-cb0976f4bb71](#) - **Name:** 'App Service apps should have remote debugging turned off'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **App Services**
3. Click on each App
4. Under **Setting** section, Click on **Configuration**
5. Under the **General settings** tab, set the **Remote debugging** option to **Off**.

Remediate from Azure CLI

To set remote debugging status to off, run the following command

```
az webapp config set --resource-group <resource_group_name> --name <app_name> -  
--remote-debugging-enabled false
```

Remediation from PowerShell

To set remote debugging status to off, run the following command

```
Set-AzWebApp -ResourceGroupName <resource_group_name> -Name <app_name> -  
RemoteDebuggingEnabled $false
```





Default Value:

By default, remote debugging is set to **off**

References:

1. <https://learn.microsoft.com/en-us/visualstudio/debugger/remote-debugging-azure-app-service>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-2-audit-and-enforce-secure-configurations>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.			
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.			

2.1.11 Ensure incoming client certificates are enabled and required (if in use) (Automated)

Profile Applicability:

- Level 2

Description:

Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app.

Rationale:

The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client with valid certificates can access the app.

Impact:

Utilizing and maintaining client certificates will require additional work to obtain and manage replacement and key rotation.

NOTE: This recommendation cannot be implemented if following the recommendation titled "Ensure 'HTTP Version' is set to '2.0' (if in use)." This recommendation should only be considered for scenarios where HTTP versions prior to 2.0 are required for an app, and mutual certificate authentication is desired for validating clients.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **App Services**
3. Click on each App
4. Under the Settings section, Click on **Configuration**, then **General settings**
5. Ensure that the option **Client certificate mode** located under Incoming client certificates is set to **Require**

Audit from Azure CLI

To check Incoming client certificates value for an existing app, run the following command,

```
az webapp show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query clientCertEnabled
```

The output should return **true** if Incoming client certificates value is set to **On**.

Audit from PowerShell

List all web apps.

```
Get-AzWebApp
```

For each web app run the following command.

```
Get-AzWebApp -ResourceGroup <app resource group> -Name <app name>
```

Make sure the **ClientCertEnabled** 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/~/%2FDefinitions

- **Policy ID:** [19dd1db6-f442-49cf-a838-b0786b4401ef](#) - **Name:** 'App Service apps should have Client Certificates (Incoming client certificates) enabled'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **App Services**
3. Click on each App
4. Under the Settings section, Click on **Configuration**, then **General settings**
5. Set the option **Client certificate mode** located under Incoming client certificates to **Require**

Remediate from Azure CLI

To set Incoming client certificates value for an existing app, run the following command:

```
az webapp update --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --set clientCertEnabled=true
```





Default Value:

By default, incoming client certificates are disabled.

References:

1. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-authenticate-server-and-services>
2. <https://learn.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>

CIS Controls:

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

2.1.12 Ensure 'App Service authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2

Description:

App Service authentication can prevent anonymous HTTP requests from reaching an app, or authenticate those with tokens before they reach the app. If an anonymous request is received from a browser, App Service will redirect to a login page. To handle the login process, a choice from a set of identity providers can be made, or a custom authentication mechanism can be implemented.

Rationale:

By enabling authentication, every incoming HTTP request passes through it before being handled by the application code. It also handles authentication of users with the specified provider (Entra ID, Facebook, Google, Microsoft Account, and Twitter), validation, storage and refreshing of tokens, managing the authenticated sessions, and injecting identity information into request headers.

Impact:

This is only required for apps that require authentication. Enabling it on a site like a marketing or support website will prevent unauthenticated access, which would be undesirable.

Adding an authentication requirement will increase costs and require additional security components to facilitate the authentication.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Authentication**.
4. Ensure that **App Service authentication** is set to **Enabled**.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the authentication setting:

For v1 auth commands:

```
az webapp auth show --resource-group <resource-group-name> --name <app-name> --query enabled
```

For v2 auth commands:

```
az webapp auth show --resource-group <resource-group-name> --name <app-name> --query properties.platform.enabled
```

Ensure that **true** is returned.

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:** [95bccee9-a7f8-4bec-9ee9-62c3473701fc](#) - **Name:** 'App Service apps should have authentication enabled'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Authentication**.
4. If an identity provider is not configured:
 1. Click **Add identity provider**.
 2. Provide appropriate configuration for an identity provider and click **Add**.
5. If **App Service authentication** is set to **Disabled**:
 1. Click **Enable authentication**.
6. Repeat steps 1-5 for each app requiring remediation.

Remediate from Azure CLI

For each app requiring remediation, run the following command to enable authentication:

```
az webapp auth update --resource-group <resource-group-name> --name <app-name> --enabled true
```

Note: In order to access **App Service authentication** settings for an app using the Microsoft API, the **Website Contributor** permission at the subscription level is required. A custom role can be created instead of **Website Contributor** to provide more specific permissions and maintain the principle of least privileged access.

Default Value:

By default, **App Service authentication** is set to **Disabled**.







References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>
2. <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#website-contributor>
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-6-define-and-implement-identity-and-privileged-access-strategy>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp/auth>

Additional Information:

You're not required to use App Service for authentication and authorization. Many web frameworks come with security features built in, and you can use them if you like. If you need more flexibility than App Service provides, you can also write your own utilities. Secure authentication and authorization require a deep understanding of security, including federation, encryption, JSON Web Token (JWT) management, grant types, and so on.

CIS Controls:

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

2.1.13 Ensure managed identities are configured (Automated)

Profile Applicability:

- Level 1

Description:

Managed identities from Microsoft Entra ID allow App Service apps to securely access other Azure services without the need to provision or rotate any secrets.

Rationale:

Using managed identities with App Service apps eliminates the need to store and manage credentials to access Azure resources.

Impact:

Minor administrative overhead to configure and manage role assignments for managed identities.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Identity**.
4. Ensure that in the **System assigned** pane, the **Status** is set to **On**, and an **Object (principal) ID** is displayed, or that in the **User assigned** pane, a managed identity is listed.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list web apps:

```
az webapp list
```

For each web app, run the following command:

```
az webapp identity show --resource-group <resource-group-name> --name <app-name> --query type
```

Ensure the command returns **SystemAssigned**, **UserAssigned**, or both.

Audit from PowerShell

Run the following command to list web apps:

```
Get-AzWebApp
```

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


```
Get-AzWebapp -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the assigned identity type for a web app:

```
$webapp.Identity.Type
```

Ensure the command returns **SystemAssigned**, **UserAssigned**, or both.

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:** [2b9ad585-36bc-4615-b300-fd4435808332](#) - **Name:** 'App Service apps should use managed identity'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Identity**.
4. To add a system assigned managed identity:
 1. In the **System assigned** pane, under **Status**, click **On**.
 2. Click **Save**.
 3. Click **Yes**.
5. To add a user assigned managed identity:
 1. In the **User assigned** pane, click **Add**.
 2. Use the filter box to search for a managed identity.
 3. Select the identity.
 4. Click **Add**.
6. Repeat steps 1-5 for each app requiring remediation.

Remediate from Azure CLI

For each web app requiring remediation, run the following command to assign a managed identity:

```
az webapp identity assign --resource-group <resource-group-name> --name <app-name>
```

Remediate from PowerShell

For each web app requiring remediation, run the following command to assign a managed identity:

```
Set-AzWebApp -AssignIdentity $True -ResourceGroupName <resource-group-name> -Name <app-name>
```





Default Value:

Managed identities are disabled by default for App Service apps.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-1-use-centralized-identity-and-authentication-system>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp>

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.			

2.1.14 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 the service is not directly exposed to the public Internet. This has the added benefit of providing more granular control over security settings and configurations for those additional layers of separation.

Impact:

NOTE: Prior to disabling public network access, it is strongly recommended that, for each App Service App, either:

- complete virtual network integration as described in **"Ensure app is integrated with a virtual network"**

OR

- set up private endpoints/links as described in **"Ensure private endpoints are used to access App Service apps."**

Disabling public network access restricts direct access to the service. This enhances security but will require the configuration of a virtual network and/or private endpoints for any services or users needing access within trusted networks.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Inbound traffic configuration**, ensure that **Public network access** is set to **Disabled**.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the public network access setting:

```
az webapp show --resource-group <resource-group-name> --name <app-name> --query "publicNetworkAccess"
```

Ensure that the command returns **"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:** [1b5ef780-c53c-4a64-87f3-bb9c8c8094ba](#) - **Name:** 'App Service apps should disable public network access'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Inbound traffic configuration**, click the text next to **Public network access**.
5. Select the radio button next to **Disabled**.
6. Click **Save**.
7. Check the box to confirm the change.
8. Click **Continue**.
9. Repeat steps 1-8 for each app requiring remediation.

Remediate from Azure CLI

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

```
az resource update --resource-group <resource-group-name> --name <app-name> --resource-type "Microsoft.Web/sites" --set properties.publicNetworkAccess=Disabled
```










Default Value:

By default, public network access is enabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/networking-features>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

2.1.15 Ensure App Service plan SKU supports private endpoints (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that your App Service plan SKU supports private endpoints. Private endpoints provide secure access over Azure Private Link, which keeps traffic on the Microsoft backbone network and eliminates exposure to the public internet. Note that not all SKUs support private endpoints.

Rationale:

An appropriately configured private endpoint eliminates public exposure and helps prevent data exfiltration.

Impact:

App Service plan costs vary based on the selected SKU.

- App Service on Linux pricing: <https://azure.microsoft.com/en-us/pricing/details/app-service/linux/>
- App Service on Windows pricing: <https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. In the **Properties** pane, under **Hosting**, next to **SKU and size**, ensure that the plan tier is one of the following: **Basic, Standard, ElasticPremium, Premium, PremiumV2, Premium0V3, PremiumV3, PremiumMV3, IsolatedV2, IsolatedMV2, WorkflowStandard, FlexConsumption**, and that the plan name is one of the following: **B1, B2, B3, S1, S2, S3, EP1, EP2, EP3, P1, P2, P3, P1V2, P2V2, P3V2, P0V3, P1V3, P2V3, P3V3, P1MV3, P2MV3, P3MV3, P4MV3, P5MV3, I1V2, I2V2, I3V2, I4V2, I5V2, I6V2, I1MV2, I2MV2, I3MV2, I4MV2, I5MV2, WS1, WS2, WS3, FC1**.
4. Repeat steps 1-3 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the App Service plan ID:

```
az webapp show --resource-group <resource-group-name> --name <app-name> --query appServicePlanId
```

For each App Service plan, run the following command to get the plan SKU tier and name:

```
az appservice plan show --resource-group <resource-group-name> --name <app-service-plan-name> --query "{tier:sku.tier,name:sku.name}"
```

Ensure that the plan tier is one of the following: **Basic, Standard, ElasticPremium, Premium, PremiumV2, Premium0V3, PremiumV3, PremiumMV3, IsolatedV2, IsolatedMV2, WorkflowStandard, FlexConsumption**, and that the plan name is one of the following: **B1, B2, B3, S1, S2, S3, EP1, EP2, EP3, P1, P2, P3, P1V2, P2V2, P3V2, P0V3, P1V3, P2V3, P3V3, P1MV3, P2MV3, P3MV3, P4MV3, P5MV3, I1V2, I2V2, I3V2, I4V2, I5V2, I6V2, I1MV2, I2MV2, I3MV2, I4MV2, I5MV2, WS1, WS2, WS3, FC1**.

Audit from PowerShell

Run the following command to list apps:

```
Get-AzWebApp
```

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

```
$app = Get-AzWebApp -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the App Service plan ID:

```
$app.ServerFarmId
```

Run the following command to get the App Service plan in a resource group with a given name:

```
$plan = Get-AzAppServicePlan -ResourceGroupname <resource-group-name> -Name <app-service-plan-name>
```

Run the following command to get the plan SKU tier and name:

```
$plan.Sku | select-object Tier, Name
```

Ensure that the plan tier is one of the following: **Basic, Standard, ElasticPremium, Premium, PremiumV2, Premium0V3, PremiumV3, PremiumMV3, IsolatedV2, IsolatedMV2, WorkflowStandard, FlexConsumption**, and that the plan name is one of the following: **B1, B2, B3, S1, S2, S3, EP1, EP2, EP3, P1, P2, P3, P1V2, P2V2, P3V2, P0V3, P1V3, P2V3, P3V3, P1MV3, P2MV3, P3MV3, P4MV3, P5MV3, I1V2, I2V2, I3V2, I4V2, I5V2, I6V2, I1MV2, I2MV2, I3MV2, I4MV2, I5MV2, WS1, WS2, WS3, FC1**.

Repeat for each app.

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:** [546fe8d2-368d-4029-a418-6af48a7f61e5](#) - **Name:** 'App Service apps should use a SKU that supports private link'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. In the **Properties** pane, under **Hosting**, next to **Name**, click the App Service plan name.
4. Under **Current App Service plan**, next to **Name**, click the App Service plan name.
5. Under **Essentials**, next to **Pricing plan**, click the pricing plan name.
6. Select a pricing plan where the plan tier is one of the following: **Basic**, **Standard**, **ElasticPremium**, **Premium**, **PremiumV2**, **Premium0V3**, **PremiumV3**, **PremiumMV3**, **IsolatedV2**, **IsolatedMV2**, **WorkflowStandard**, **FlexConsumption**, and the plan name is one of the following: **B1**, **B2**, **B3**, **S1**, **S2**, **S3**, **EP1**, **EP2**, **EP3**, **P1**, **P2**, **P3**, **P1V2**, **P2V2**, **P3V2**, **P0V3**, **P1V3**, **P2V3**, **P3V3**, **P1MV3**, **P2MV3**, **P3MV3**, **P4MV3**, **P5MV3**, **I1V2**, **I2V2**, **I3V2**, **I4V2**, **I5V2**, **I6V2**, **I1MV2**, **I2MV2**, **I3MV2**, **I4MV2**, **I5MV2**, **WS1**, **WS2**, **WS3**, **FC1**.
7. Click **Select**.
8. Click **Downgrade** or **Upgrade** to confirm the change.
9. Repeat steps 1-8 for each app and App Service plan requiring remediation.

Remediate from Azure CLI

For each App Service plan requiring remediation, run the following command to update the SKU:

```
az appservice plan update --resource-group <resource-group-name> --name <app-service-plan-name> --sku <sku>
```

Default Value:





The App Service plan is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-private-endpoint>

3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/cli/azure/appservice/plan>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
6. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azappserviceplan>
7. <https://azure.microsoft.com/en-us/pricing/details/app-service/linux/>
8. <https://azure.microsoft.com/en-us/pricing/details/app-service/windows/>

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).			

2.1.16 Ensure private endpoints are used to access App Service apps (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:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Inbound traffic configuration**, click the link next to **Private endpoints**.
5. Ensure that at least one private endpoint is listed with a **Connection state** of **Approved**.
6. Repeat steps 1-5 for each app.

Audit from Azure CLI

Run the following command to list apps IDs:

```
az webapp list --query [*].id
```

Run the following command to list private link service IDs and connection states:

```
az network private-endpoint list --query  
[*].privateLinkServiceConnections[*].[privateLinkServiceId,privateLinkService  
ConnectionState.status]
```

Ensure that a private endpoint exists for each app with a connection state of **Approved**.

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:** [687aa49d-0982-40f8-bf6b-66d1da97a04b](#) - **Name:** 'App Service apps should use private link'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Inbound traffic configuration**, click the link next to **Private endpoints**.
5. Click **+ Add**.
6. From the drop-down menu, select **Express** or **Advanced**.
7. If selecting **Express**:
 1. Provide a **Name**, and select a **Subscription**, **Virtual network**, and **Subnet**.
 2. Click **OK**.
8. If selecting **Advanced**:
 1. Select a **Subscription** and **Resource group**, provide an instance **Name** and **Network Interface Name**, and select a **Region**.
 2. Click **Next : Resource >**.
 3. Select a **Target sub-resource**.
 4. Click **Next : Virtual Network >**.
 5. Select a **Virtual network** and a **Subnet**.
 6. Click **Next : DNS >**.
 7. Optionally update the DNS configuration.
 8. Click **Next : Tags >**.
 9. Optionally configure tags.
 10. Click **Next : Review + create >**.
 11. Click **Create**.

Remediate from Azure CLI

For each app requiring remediation, run the following command to create a private endpoint:

```
az network private-endpoint create --resource-group <resource-group-name> --location <location> --name <private-endpoint-name> --vnet-name <virtual-network-name> --subnet <subnet-name> --private-connection-resource-id <fully-qualified-app-id> --connection-name <connection-name> --group-id sites
```





Default Value:

By default, private endpoints are not configured for apps.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-private-endpoint>
2. <https://azure.microsoft.com/en-us/pricing/details/private-link/>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/cli/azure/network/private-endpoint>

CIS Controls:

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

2.1.17 Ensure private endpoints used to access App Service apps use private DNS zones (Manual)

Profile Applicability:

- Level 2

Description:

Use private DNS zones to override DNS resolution for a private endpoint. A private DNS zone links a virtual network to an App Service app.

This recommendation assumes application of, and should be applied in conjunction with, the recommendation titled "Ensure private endpoints are used to access App Service apps."

Rationale:

It's important to correctly configure DNS settings to ensure that the fully qualified domain name (FQDN) of the App Service app resolves to the private endpoint IP address.

Impact:

Incorrectly configured DNS settings may result in unintentional exposure of traffic to the public internet.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Inbound traffic configuration**, click the link next to **Private endpoints**.
5. Click the name of a private endpoint.
6. Under **Settings**, click **DNS configuration**.
7. Ensure a configuration is displayed with a value for **Private DNS zone**.
8. Repeat steps 1-7 for each app and private endpoint.

Remediation:

Remediate from Azure Portal





1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.

4. Under **Inbound traffic configuration**, click the link next to **Private endpoints**.
5. Click the name of a private endpoint.
6. Under **Settings**, click **DNS configuration**.
7. Click **+ Add configuration**.
8. Select a **Subscription**, **Private DNS zone**, and provide a **DNS zone group** and **Configuration name**.
9. Click **Add**.
10. Repeat steps 1-9 for each app and private endpoint requiring remediation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-private-endpoint#dns>
2. <https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns>

CIS Controls:

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

2.1.18 Ensure app is integrated with a virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Integrate App Service apps with a virtual network to enable access to resources in or through a non-internet-routable virtual network.

Rationale:

Integrate App Service apps with a virtual network for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, ensure that a virtual network and subnet name are displayed.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the virtual network subnet ID:

```
az webapp show --resource-group <resource-group-name> --name <app-name> --  
query "virtualNetworkSubnetId"
```

Ensure that a virtual network subnet ID is returned.

Audit from PowerShell

Run the following command to list apps:

```
Get-AzWebApp
```

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

```
$app = Get-AzWebapp -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the virtual network subnet ID:

```
$app.virtualNetworkSubnetId
```

Ensure that a virtual network subnet ID is returned.

Repeat for each app.

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:** [72d04c29-f87d-4575-9731-419ff16a2757](#) - **Name:** 'App Service apps should be injected into a virtual network'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, click **Not configured**.
5. Click **Add virtual network integration**.
6. Select an existing App Service Plan connection, or select **New connection** and select a subscription, virtual network, and subnet.
7. Click **Connect**.
8. Repeat steps 1-7 for each app requiring remediation.

Remediate from Azure CLI

For each app requiring remediation, run the following command to integrate with a virtual network:

```
az webapp vnet-integration add --resource-group <resource-group-name> --name <app-name> --vnet <virtual-network-name> --subnet <subnet-name>
```

Remediate from PowerShell

For each app requiring remediation, run the following commands to integrate with a virtual network:

Prepare parameters:


```
$siteName = '<app-name>'
$virtualNetworkResourceGroupName = '<virtual-network-resource-group-name>'
$appResourceGroupName = '<app-resource-group-name>'
$virtualNetworkName = '<virtual-network-name>'
$integrationSubnetName = '<subnet-name>'
$virtualNetworkSubscriptionId = '<subscription-guid>'
```

Check if the subnet is delegated to **Microsoft.Web/serverFarms**:

```
$vnet = Get-AzVirtualNetwork -Name $virtualNetworkName -ResourceGroupName
$virtualNetworkResourceGroupName
$subnet = Get-AzVirtualNetworkSubnetConfig -Name $integrationSubnetName -
VirtualNetwork $vnet
Get-AzDelegation -Subnet $subnet
```

Add delegation:

```
$subnet = Add-AzDelegation -Name "myDelegation" -ServiceName
"Microsoft.Web/serverFarms" -Subnet $subnet
Set-AzVirtualNetwork -VirtualNetwork $vnet
```

Configure virtual network integration:

```
$subnetResourceId =
"/subscriptions/$virtualNetworkSubscriptionId/resourceGroups/$virtualNetworkResourceGroupName/pro
viders/Microsoft.Network/virtualNetworks/$virtualNetworkName/subnets/$integrationSubnet
Name"
$app = Get-AzResource -ResourceType Microsoft.Web/sites -ResourceGroupName
$appResourceGroupName -ResourceName $siteName
$app.Properties.virtualNetworkSubnetId = $subnetResourceId
$app.Properties.vnetRouteAllEnabled = 'true'
$app | Set-AzResource -Force
```





Default Value:

By default, virtual network integration is not configured.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>
2. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-enable>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>

CIS Controls:

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

2.1.19 Ensure configuration is routed through the virtual network integration (Automated)

Profile Applicability:

- Level 2

Description:

By default, configuration traffic for App Service apps goes directly over the public route. Container image pulls and content sharing can be routed through the virtual network integration.

This recommendation should be applied after integrating an App Service app with a virtual network.

Rationale:

Route container image pulls and content sharing through a virtual network integration for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the container image share and content share settings:

```
az webapp show --resource-group <resource-group-name> --name <app-name> --query "[vnetImagePullEnabled,vnetContentShareEnabled]"
```

Ensure that **[true,true]** is returned.

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:** [801543d1-1953-4a90-b8b0-8cf6d41473a5](#) - **Name:** 'App Service apps should enable configuration routing to Azure Virtual Network'

Remediation:

Remediate from Azure CLI

For each app requiring remediation, run the following command to route container image pulls and content sharing through the virtual network integration:

```
az resource update --resource-group <resource-group-name> --name <app-name> -  
-resource-type "Microsoft.Web/sites" --set  
properties.vnetImagePullEnabled=true --set  
properties.vnetContentShareEnabled=true
```

Default Value:

By default, configuration traffic goes directly over the public route.





References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#routes>
2. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-configuration-routing>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

Additional Information:

In addition to configuring the routing for content sharing, you must also ensure that any firewall or Network Security Group configured on traffic from the subnet allow traffic to port 443 and 445.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 <u>Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.1.20 Ensure all traffic is routed through the virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Enable `vnetRouteAllEnabled` to ensure all outbound traffic is routed through the integrated virtual network.

This recommendation should be applied after integrating an App Service app with a virtual network.

Rationale:

Routing all outbound traffic through the virtual network enhances security.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
5. Under **Application routing**, ensure that the box next to **Outbound internet traffic** is checked.
6. Repeat steps 1-5 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the virtual network traffic routing setting:

```
az webapp show --resource-group <resource-group-name> --name <app-name> --query vnetRouteAllEnabled
```

Ensure that `true` is returned.

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:** [a691eacb-474d-47e4-b287-b4813ca44222](#) - **Name:** 'App Service apps should enable outbound non-RFC 1918 traffic to Azure Virtual Network'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
5. Under **Application routing**, check the box next to **Outbound internet traffic**.
6. Click **Apply**.
7. Repeat steps 1-6 for each app requiring remediation.

Remediate from Azure CLI

For each app requiring remediation, run the following command to route all traffic through the virtual network:

```
az resource update --resource-group <resource-group-name> --name <app-name> -  
-resource-type "Microsoft.Web/sites" --set  
properties.vnetRouteAllEnabled=true
```





Default Value:

For apps integrated with a virtual network, all traffic is routed through the virtual network by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-application-routing>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>13.4 Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.1.21 Ensure cross-origin resource sharing does not allow all origins (Automated)

Profile Applicability:

- Level 2

Description:

Cross-origin resource sharing (CORS) is a security feature that controls how applications interact with resources hosted on different domains.

Rationale:

Restrict CORS to only trusted origins to help enforce proper access control and reduce exposure to malicious cross-origin requests.

Impact:

Configuration is required to ensure that the appropriate origins have access.

Setting up a proper CORS policy can be fairly complex and an incorrect setting could permit Cross-Site Request Forgery (CSRF). The "caveat" is that if the app being deployed is a PUBLIC API, a wildcard "*" CORS policy is absolutely necessary.

Audit:

Audit from Azure Portal

1. Go to **App Service**.
2. Click the name of an app.
3. Under **API**, click **CORS**.
4. Ensure **Allowed Origins** does not include *****.
5. Repeat steps 1-4 for each app.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to get the CORS allowed origins setting:

```
az webapp show --resource-group <resource-group-name> --name <app-name> --query siteConfig.cors.allowedOrigins
```

Ensure that the response does not include *****.

Audit from PowerShell

Run the following command to list apps:


```
Get-AzWebApp
```

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

```
$app = Get-AzWebapp -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the CORS allowed origins setting:

```
$app.SiteConfig.Cors.AllowedOrigins
```

Ensure that the response does not include *****.
Repeat for each app.

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:** [5744710e-cc2f-4ee8-8809-3b11e89f4bc9](#) - **Name:** 'App Service apps should not have CORS configured to allow every resource to access your apps'

Remediation:

Remediate from Azure Portal

1. Go to **App Service**.
2. Click the name of an app.
3. Under **API**, click **CORS**.
4. Under **Allowed Origins**, delete the entry that equals *****.
5. Specify the origins that should be allowed to make cross-origin calls.
6. Click **Save**.
7. Repeat steps 1-6 for each app requiring remediation.

Remediate from Azure CLI

For each app requiring remediation, run the following command:

```
az webapp cors remove --resource-group <resource-group-name> --name <app-name> --allowed-origins ""
```

Use the following command to specify the origins that should be allowed:

```
az webapp cors add --resource-group <resource-group-name> --name <app-name> --allowed-origins <allowed-origins>
```





Default Value:

By default, CORS is not configured.

References:

1. <https://learn.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-rest-api>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp/cors>
3. <https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers-Cheat-Sheet.html>
4. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CORS>
5. <https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site-Request-Forgery-Prevention-Cheat-Sheet.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.1 Establish and Maintain a Secure Application Development Process Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	18.1 Establish Secure Coding Practices Establish secure coding practices appropriate to the programming language and development environment being used.			

2.2 App Service Deployment Slots

2.2.1 Ensure 'Java version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Java may be deprecated and no longer supported. Using a supported version of Java for App Service deployment slots is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of currently supported versions of Java here:

<https://www.oracle.com/java/technologies/java-se-support-roadmap.html>

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, ensure that for a **Stack** of **Java**, the **Major version** reflects a currently supported release, and that the **Java web server version** is set to the **auto-update** option.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the Java version:

```
az resource show --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --query properties.[javaContainer,javaContainerVersion,javaVersion,linuxFxVersion,windowsFxVersion]
```

If Java is in use, ensure the version is currently supported.

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:** [46dad49f-8945-44d7-9bb1-2e1542f627d3](#) - **Name:** 'App Service app slots that use Java should use a specified 'Java version''

Remediation:

Note: No action is required if Java is not in use.

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, for a **Stack of Java**, set the **Major version** to a currently supported release, and set the **Java web server version** to the **auto-update** option.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az webapp list-runtimes
```

For each deployment slot requiring remediation, run the following command with the appropriate parameters to update the Java version:

```
az resource update --name web --resource-group <resource-group-name> --
namespace Microsoft.Web --resource-type config --parent sites/<app-
name>/slots/<deployment-slot-name> --set
properties.[javaContainer|javaContainerVersion|javaVersion|linuxFxVersion|win
dowsFxVersion]="<java-container|java-container-version|java-version|java-
runtime-version>"
```







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-language-java-deploy-run>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://www.oracle.com/java/technologies/java-se-support-roadmap.html>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp>
6. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.2.2 Ensure 'Python version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Python may be deprecated and no longer supported. Using a supported version of Python for App Service deployment slots is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions (given a status of "security") of Python here: <https://devguide.python.org/versions/>

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, ensure that for a **Stack** of **Python**, the **Major version** and **Minor version** reflect a currently supported release.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the Python version:

```
az resource show --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --query properties.[linuxFxVersion,pythonVersion,windowsFxVersion]
```

If Python is in use, ensure the version is currently supported.

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:** [9c014953-ef68-4a98-82af-fd0f6b2306c8](#) - **Name:** 'App Service app slots that use Python should use a specified 'Python version''

Remediation:

Note: No action is required if Python is not in use.

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, for a **Stack** of **Python**, set the **Major version** and **Minor version** to a currently supported release.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az webapp list-runtimes
```

For each deployment slot requiring remediation, run the following command with the appropriate parameters to update the Python version:

```
az resource update --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --set properties.[linuxFxVersion|windowsFxVersion]="PYTHON|<python-version>"
```








Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#configure-language-stack-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://devguide.python.org/versions/>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp>
6. <https://learn.microsoft.com/en-us/cli/azure/resource>

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.			

2.2.3 Ensure 'PHP version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of PHP may be deprecated and no longer supported. Using a supported version of PHP for App Service deployment slots is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions of PHP here:

<https://www.php.net/supported-versions.php>

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, ensure that for a **Stack** of **PHP**, the **Major version** and **Minor version** reflect a currently supported release.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the PHP version:

```
az resource show --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --query properties.[linuxFxVersion,phpVersion]
```

If PHP is in use, ensure the version is currently supported.

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:** [f466b2a6-823d-470d-8ea5-b031e72d79ae](#) - **Name:** 'App Service app slots that use PHP should use a specified 'PHP version''

Remediation:

Note: No action is required if PHP is not in use.

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, for a **Stack** of **PHP**, set the **Major version** and **Minor version** to a currently supported release.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az webapp list-runtimes
```

For each deployment slot requiring remediation, run the following command with the appropriate parameters to update the PHP version:

```
az resource update --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --set properties.[linuxFxVersion|phpVersion]="<python-runtime-version|python-version>"
```







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#general-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://www.php.net/supported-versions.php>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp>
6. <https://learn.microsoft.com/en-us/cli/azure/resource>

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.			

2.2.4 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

Basic Authentication Publishing Credentials provides the ability to publish—or deploy to—an App Service deployment slot without a centralized Identity Provider. For a more effective, capable, and secure solution for Identity, Authentication, Authorization, and Accountability, a centralized Identity Provider such as Entra ID is strongly advised.

Rationale:

Basic Authentication introduces an identity silo for privileged access to a resource and produces logging which may not provide a full chain of accountability. This can be exploited in numerous ways and represents a significant vulnerability and attack vector.

Impact:

Disabling 'Basic Auth Publishing Credentials' will prevent the following deployment methods from working:

FTP Basic Auth Publishing Credentials:

- FTP
- FTPS

SCM Basic Auth Publishing Credentials:

- Local Git
- GitHub
- Azure Repos
- Bitbucket
- Visual Studio (Version 17.12 and earlier)

If this recommendation cannot be implemented because one of the above listed deployment methods is necessary and cannot be adapted, compensating controls (e.g. using FTPS Only and disabling only "SCM Basic Auth Publishing Credentials") are recommended to reduce potential attack surface.

An Identity Provider that can be used by the App Service deployment slot for authenticating users is required.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** tab, under **Platform settings**, ensure that **SCM Basic Auth Publishing Credentials** and **FTP Basic Auth Publishing Credentials** are set to **Off**.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the basic authentication for FTP setting:

```
az resource show --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name>/slots/<deployment-slot-name> --query properties.allow
```

Ensure that **false** is returned.

For each deployment slot, run the following command to get the basic authentication for SCM setting:

```
az resource show --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name>/slots/<deployment-slot-name> --query properties.allow
```

Ensure that **false** is returned.

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:** [ec71c0bc-6a45-4b1f-9587-80dc83e6898c](#) - **Name:** 'App Service app slots should have local authentication methods disabled for FTP deployments'
- **Policy ID:** [847ef871-e2fe-4e6e-907e-4adbf71de5cf](#) - **Name:** 'App Service app slots should have local authentication methods disabled for SCM site deployments'

Remediation:

CAUTION: Applying changes may cause your App Service resource to restart.
Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** tab, under **Platform settings**, set **SCM Basic Auth Publishing Credentials** and **FTP Basic Auth Publishing Credentials** to **Off**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to disable basic authentication for FTP:

```
az resource update --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name>/slots/<deployment-slot-name> --set properties.allow=false
```

For each deployment slot requiring remediation, run the following command to disable basic authentication for SCM:

```
az resource update --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<app-name>/slots/<deployment-slot-name> --set properties.allow=false
```





Default Value:

Basic authentication is enabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-basic-auth-disable>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.2.5 Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

By default, App Service supports deployment over FTP. If FTP is essential for a deployment workflow, FTPS should be enforced for all App Service deployment slots.

If FTPS is not explicitly required, the recommended setting is **Disabled**.

Rationale:

FTP is an unencrypted network protocol that transmits data—including passwords—in clear text. The use of this protocol can lead to both data and credential compromise and can present opportunities for exfiltration, persistence, and lateral movement.

Impact:

Deployment workflows that rely on FTP or FTPS rather than WebDeploy or HTTPS endpoints may be affected.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment Slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **FTP state** is set to **FTPS only** or **Disabled**.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the FTPS state setting:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<app-  
name>/slots/<deployment-slot-name> --query properties.ftpState
```

Ensure that "FtpsOnly" or "Disabled" is returned.

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:** [c285a320-8830-4665-9cc7-bbd05fc7c5c0](#) - **Name:** 'App Service app slots should require FTPS only'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment Slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, set **FTP state** to **FTPS only** or **Disabled**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to set FTPS state to **FtpsOnly** or **Disabled**:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<app-  
name>/slots/<deployment-slot-name> --set  
properties.ftpState=<FtpsOnly|Disabled>
```

Default Value:





By default, FTP state is set to **FTPS only**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/deploy-ftp>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-security>
3. <https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/create-or-update-configuration#ftpstate>

4. <https://learn.microsoft.com/en-us/cli/azure/webapp>
5. <https://learn.microsoft.com/en-us/cli/azure/resource>
6. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit>
7. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>

CIS Controls:

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

2.2.6 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for HTTP, either due to security flaws or to include additional functionalities. Using the latest HTTP version allows apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.

Rationale:

Newer versions may contain security enhancements and additional functionalities. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

HTTP 2.0 has additional performance improvements for the head-of-line blocking problem of the old HTTP version, header compression, and request prioritization. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient mechanisms for data streaming.

Impact:

Most modern browsers support the HTTP/2 protocol over TLS only, while non-encrypted traffic continues to use HTTP/1.1. To ensure that client browsers connect to your app with HTTP/2, either purchase an App Service Certificate for your app's custom domain or bind a third-party certificate.

NOTE: HTTP/2 cannot be used in tandem with mutual authentication or client certificates.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **HTTP version** is set to **2.0**.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the **http20Enabled** setting:

```
az resource show --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --query properties.http20Enabled
```

Ensure that **true** is returned.

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:** [4dcfb8b5-05cd-4090-a931-2ec29057e1fc](#) - **Name:** 'App Service app slots should use latest 'HTTP Version''

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, set **HTTP version** to **2.0**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable **http20Enabled**:

```
az resource update --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --set properties.http20Enabled=true
```







Default Value:

By default, HTTP version is set to 1.1.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#general-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://learn.microsoft.com/en-us/cli/azure/webapp>
5. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.2.7 Ensure 'HTTPS Only' is set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

Azure App Service allows deployment slots to run under both HTTP and HTTPS by default. Deployment slots can be accessed by anyone using non-secure HTTP links by default. Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic.

Rationale:

Enabling HTTPS-only traffic will redirect all non-secure HTTP requests to HTTPS ports. HTTPS uses the TLS/SSL protocol to provide a secure connection which is both encrypted and authenticated. It is therefore important to support HTTPS for the security benefits.

Impact:

When it is enabled, every incoming HTTP request is redirected to the HTTPS port. This means an extra level of security will be added to the HTTP requests made to the deployment slot.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** tab, under **Platform settings**, ensure that **HTTPS Only** is set to **On**.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that **httpsOnly** is set to **true**.

Audit from PowerShell

Run the following command to list apps:

```
Get-AzWebApp
```

Run the following command to list deployment slots for an app:

```
Get-AzWebAppSlot -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the deployment slot with a given name:

```
$slot = Get-AzWebAppSlot -ResourceGroupName <resource-group-name> -Name <app-name> -Slot <deployment-slot-name>
```

Run the following command to get the HTTPS setting for the deployment slot:

```
$slot.httpsOnly
```

Ensure that the command returns **True**.
Repeat for each app and deployment slot.

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:** [ae1b9a8c-dfce-4605-bd91-69213b4a26fc](#) - **Name:** 'App Service app slots should only be accessible over HTTPS'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** tab, under **Platform settings**, next to **HTTPS Only**, select the radio button next to **On**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable **HTTPS Only**:

```
az resource update --resource-group <resource-group-name> --name <app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.httpsOnly=true
```

Remediate from PowerShell

For each deployment slot requiring remediation, run the following command to enable **HTTPS Only**:

```
Set-AzWebAppSlot -ResourceGroupName <resource-group-name> -Name <app-name> -Slot <deployment-slot-name> -HttpsOnly $true
```





Default Value:

HTTPS Only is disabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-security#https-and-certificates>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://techcommunity.microsoft.com/t5/azure-paas-blog/enable-https-setting-on-azure-app-service-using-azure-policy/ba-p/3286603>
4. <https://learn.microsoft.com/en-us/cli/azure/webapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebappslot>
6. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebappslot>
7. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.2.8 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)

Profile Applicability:

- Level 1

Description:

The TLS (Transport Layer Security) protocol secures the transmission of data over the internet using standard encryption technology. App Service deployment slots use TLS 1.2 for the **Minimum Inbound TLS Version** by default and allow for the use of TLS versions 1.0, 1.1, and 1.3. NIST strongly suggests the use of TLS 1.2 and recommends the adoption of TLS 1.3.

Rationale:

TLS 1.0 and 1.1 are outdated and vulnerable to security risks. Since TLS 1.2 and TLS 1.3 provide enhanced security and improved performance, it is highly recommended to use TLS 1.2 or higher whenever possible.

Impact:

Using the latest TLS version may affect compatibility with clients and backend services.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **Minimum Inbound TLS Version** is set to **1.2** or higher.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the TLS version setting:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<app-  
name>/slots/<deployment-slot-name> --query properties.minTlsVersion
```

Ensure that "1.2" or higher is returned.

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:** [4ee5b817-627a-435a-8932-116193268172](#) - **Name:** 'App Service app slots should use the latest TLS version'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, click the drop-down next to **Minimum Inbound TLS Version** and select **1.2** or higher.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to update the TLS version:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<app-  
name>/slots/<deployment-slot-name> --set properties.minTlsVersion=<1.2|1.3>
```

Default Value:





By default, TLS version is set to 1.2.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-bindings#how-can-i-change-the-minimum-tls-versions-for-the-app>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit>

3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-8-detect-and-disable-insecure-services-and-protocols>
4. <https://learn.microsoft.com/en-us/cli/azure/webapp>
5. <https://learn.microsoft.com/en-us/cli/azure/resource>
6. <https://csrc.nist.gov/news/2019/nist-publishes-sp-800-52-revision-2>

CIS Controls:

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

2.2.9 Ensure end-to-end TLS encryption is enabled (Automated)

Profile Applicability:

- Level 1

Description:

End-to-end (E2E) TLS encryption ensures that front-end to worker communication within App Service deployment slots is encrypted using TLS. Without this feature, while incoming HTTPS requests are encrypted to the front ends, the traffic from front ends to workers running the application workloads would travel unencrypted inside Azure's infrastructure.

Rationale:

E2E TLS helps ensure full encryption of traffic between:

- Clients and front ends
- Front ends and worker processes hosting the application

Impact:

Enabling end-to-end TLS encryption may introduce minimal latency and require additional configuration of certificates and HTTPS settings to ensure compatibility.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **Enable end-to-end TLS encryption** is set to **On**.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that **endToEndEncryptionEnabled** 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:** [123aed70-491a-4f07-a569-e1f3a8dd651e](#) - **Name:** 'App Service app slots should enable end to end encryption'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, next to **Enable end-to-end TLS encryption**, click the radio button next to **On**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable end-to-end TLS encryption:

```
az resource update --resource-group <resource-group-name> --name <app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.endToEndEncryptionEnabled=true
```





Default Value:

By default, end-to-end TLS encryption is disabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-tls#end-to-end-tls-encryption>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.2.10 Ensure 'Remote debugging' is set to 'Off' (Automated)

Profile Applicability:

- Level 1

Description:

Remote debugging allows an App Service deployment slot to be debugged in real-time directly in the Azure environment. When remote debugging is enabled, it opens a communication channel that could potentially be exploited by unauthorized users if not properly secured.

Rationale:

Disabling remote debugging on an App Service deployment slot is primarily about enhancing security.

Remote debugging opens a communication channel that can be exploited by attackers. By disabling it, you reduce the number of potential entry points for unauthorized access.

If remote debugging is enabled without proper access controls, it can allow unauthorized users to connect to your deployment slot, potentially leading to data breaches or malicious code execution.

During a remote debugging session, sensitive information might be exposed. Disabling remote debugging helps ensure that such data remains secure. This minimizes the use of remote access tools to reduce risk.

Impact:

You will not be able to connect to your deployment slot from a remote location to diagnose and fix issues in real-time. You will not be able to step through code, set breakpoints, or inspect variables and the call stack while the deployment slot is running on the server. Remote debugging is particularly useful for diagnosing issues that only occur in the production environment. Without it, you will need to rely on logs and other diagnostic tools.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Debugging**, ensure that **Remote debugging** is set to **Off**.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the remote debugging setting:

```
az resource show --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --query properties.remoteDebuggingEnabled
```

Ensure that **false** is returned.

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/~/%2FDefinitions

- **Policy ID:** [a08ae1ab-8d1d-422b-a123-df82b307ba61](#) - **Name:** 'App Service app slots should have remote debugging turned off'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Debugging**, set **Remote debugging** to **Off**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to disable remote debugging:

```
az resource update --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --set properties.remoteDebuggingEnabled=false
```





Default Value:

By default, remote debugging is set to **off**.

References:

1. <https://learn.microsoft.com/en-us/visualstudio/debugger/remote-debugging-azure-app-service>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-2-audit-and-enforce-secure-configurations>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.			
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.			

2.2.11 Ensure incoming client certificates are enabled and required (if in use) (Automated)

Profile Applicability:

- Level 2

Description:

Client certificates allow for the deployment slot to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the deployment slot.

Rationale:

The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client with valid certificates can access the deployment slot.

Impact:

Utilizing and maintaining client certificates will require additional work to obtain and manage replacement and key rotation.

NOTE: This recommendation cannot be implemented if following the recommendation titled "Ensure 'HTTP Version' is set to '2.0' (if in use)." This recommendation should only be considered for scenarios where HTTP versions prior to 2.0 are required for a deployment slot, and mutual certificate authentication is desired for validating clients.

Audit:

From Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Incoming client certificates**, ensure that **Client certificate mode** is set to **Required**.
7. Repeat steps 1-6 for each app and deployment slot.

From Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that **clientCertEnabled** is set to **true**, and **clientCertMode** is set to **Required**.

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:** [5b0bd968-5cb5-4513-8987-27786c6f0df8](#) - **Name:** 'App Service app slots should have Client Certificates (Incoming client certificates) enabled'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Incoming client certificates**, set **Client certificate mode** to **Required**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable and require incoming client certificates:

```
az resource update --resource-group <resource-group-name> --name <app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.clientCertEnabled=true --set properties.clientCertMode=Required
```







Default Value:

By default, incoming client certificates are disabled.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-authenticate-server-and-services>
2. <https://learn.microsoft.com/en-gb/azure/app-service/app-service-web-configure-tls-mutual-auth>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.2.12 Ensure managed identities are configured (Automated)

Profile Applicability:

- Level 1

Description:

Managed identities from Microsoft Entra ID allow App Service deployment slots to securely access other Azure services without the need to provision or rotate any secrets.

Rationale:

Using managed identities with App Service deployment slots eliminates the need to store and manage credentials to access Azure resources.

Impact:

Minor administrative overhead to configure and manage role assignments for managed identities.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Identity**.
6. Ensure that in the **System assigned** pane, the **Status** is set to **On**, and an **Object (principal) ID** is displayed, or that in the **User assigned** pane, a managed identity is listed.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that **identity** contains **type** set to **SystemAssigned**, **UserAssigned**, or both.

Audit from PowerShell

Run the following command to list apps:

```
Get-AzWebApp
```

Run the following command to list deployment slots for an app:

```
Get-AzWebAppSlot -ResourceGroupName <resource-group-name> -Name <app-name>
```

Run the following command to get the deployment slot with a given name:

```
$slot = Get-AzWebAppSlot -ResourceGroupName <resource-group-name> -Name <app-name> -Slot <deployment-slot-name>
```

Run the following command to get the identity type setting for the deployment slot:

```
$slot.identity.Type
```

Ensure the command returns **SystemAssigned**, **UserAssigned**, or both.
Repeat for each app and deployment slot.

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:** [4a15c15f-90d5-4a1f-8b63-2903944963fd](#) - **Name:** 'App Service app slots should use managed identity'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Identity**.
6. To add a system assigned managed identity:
 1. In the **System assigned** pane, under **Status**, click **On**.
 2. Click **Save**.
 3. Click **Yes**.
7. To add a user assigned managed identity:
 1. In the **User assigned** pane, click **Add**.
 2. Use the filter box to search for a managed identity.
 3. Select the identity.
 4. Click **Add**.
8. Repeat steps 1-7 for each app and deployment slot requiring remediation.

Remediate from PowerShell

For each deployment slot requiring remediation, run the following command to assign a system-assigned managed identity:

```
Set-AzWebAppSlot -ResourceGroupName <resource-group-name> -Name <app-name> -Slot <deployment-slot-name> -AssignIdentity $true
```





Default Value:

Managed identities are disabled by default for App Service deployment slots.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management/im-1-use-centralized-identity-and-authentication-system>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.websites/get-azwebappslot>
6. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebappslot>

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.			

2.2.13 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 the service is not directly exposed to the public Internet. This has the added benefit of providing more granular control over security settings and configurations for those additional layers of separation.

Impact:

NOTE: Prior to disabling public network access, it is strongly recommended that, for each App Service deployment slot, either:

- complete virtual network integration as described in **"Ensure app is integrated with a virtual network"**

OR

- set up private endpoints/links as described in **"Ensure private endpoints are used to access App Service apps."**

Disabling public network access restricts direct access to the service. This enhances security but will require the configuration of a virtual network and/or private endpoints for any services or users needing access within trusted networks.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Inbound traffic configuration**, ensure that **Public network access** is set to **Disabled**.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that **publicNetworkAccess** 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:** [701a595d-38fb-4a66-ae6d-fb3735217622](#) - **Name:** 'App Service app slots should disable public network access'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Inbound traffic configuration**, click the text next to **Public network access**.
7. Select the radio button next to **Disabled**.
8. Click **Save**.
9. Check the box to confirm the change.
10. Click **Continue**.
11. Repeat steps 1-10 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to disable public network access:

```
az resource update --resource-group <resource-group-name> --name <app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.publicNetworkAccess=Disabled
```







Default Value:

By default, public network access is enabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/networking-features>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.2.14 Ensure deployment slot is integrated with a virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Integrate App Service deployment slots with a virtual network to enable access to resources in or through a non-internet-routable virtual network.

Rationale:

Integrate App Service deployment slots with a virtual network for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, ensure that a virtual network and subnet name are displayed.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that **virtualNetworkSubnetId** is set to a virtual network subnet ID.

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:** [24b7a1c6-44fe-40cc-a2e6-242d2ef70e98](#) - **Name:** 'App Service app slots should be injected into a virtual network'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, click **Not configured**.
7. Click **Add virtual network integration**.
8. Select an existing App Service Plan connection, or select **New connection** and select a subscription, virtual network, and subnet.
9. Click **Connect**.
10. Repeat steps 1-9 for each app and deployment slot requiring remediation.





Default Value:

By default, virtual network integration is not configured.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>
2. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-enable>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/cli/azure/webapp/deployment/slot>

CIS Controls:

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

2.2.15 Ensure configuration is routed through the virtual network integration (Automated)

Profile Applicability:

- Level 2

Description:

By default, configuration traffic for App Service deployment slots goes directly over the public route. Container image pulls and content sharing can be routed through the virtual network integration.

This recommendation should be applied after integrating an App Service deployment slot with a virtual network.

Rationale:

Route container image pulls and content sharing through a virtual network integration for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that **vnetImagePullEnabled** and **vnetContentShareEnabled** are 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:** [5747353b-1ca9-42c1-a4dd-b874b894f3d4](#) - **Name:** 'App Service app slots should enable configuration routing to Azure Virtual Network'

Remediation:

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to route container image pulls and content sharing through the virtual network integration:

```
az resource update --resource-group <resource-group-name> --name <app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.vnetImagePullEnabled=true --set properties.vnetContentShareEnabled=true
```

Default Value:

By default, configuration traffic goes directly over the public route.





References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#routes>
2. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-configuration-routing>
3. <https://learn.microsoft.com/en-us/cli/azure/webapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

Additional Information:

In addition to configuring the routing for content sharing, you must also ensure that any firewall or Network Security Group configured on traffic from the subnet allow traffic to port 443 and 445.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 <u>Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.16 Ensure all traffic is routed through the virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Enable `vnetRouteAllEnabled` to ensure all outbound traffic is routed through the integrated virtual network.

This recommendation should be applied after integrating an App Service deployment slot with a virtual network.

Rationale:

Routing all outbound traffic through the virtual network enhances security.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
7. Under **Application routing**, ensure that the box next to **Outbound internet traffic** is checked.
8. Repeat steps 1-7 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, ensure that `vnetRouteAllEnabled` 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:** [f5c0bfb3-acea-47b1-b477-b0edcdf6edc1](#) - **Name:** 'App Service app slots should enable outbound non-RFC 1918 traffic to Azure Virtual Network'

Remediation:

Remediate from Azure Portal

1. Go to **App Services**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
7. Under **Application routing**, check the box next to **Outbound internet traffic**.
8. Click **Apply**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to route all traffic through the virtual network:

```
az resource update --resource-group <resource-group-name> --name <app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.vnetRouteAllEnabled=true
```





Default Value:

For deployment slots integrated with a virtual network, all traffic is routed through the virtual network by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-application-routing>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>13.4 Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.17 Ensure cross-origin resource sharing does not allow all origins (Automated)

Profile Applicability:

- Level 2

Description:

Cross-origin resource sharing (CORS) is a security feature that controls how applications interact with resources hosted on different domains.

Rationale:

Restrict CORS to only trusted origins to help enforce proper access control and reduce exposure to malicious cross-origin requests.

Impact:

Configuration is required to ensure that the appropriate origins have access.

Setting up a proper CORS policy can be fairly complex and an incorrect setting could permit Cross-Site Request Forgery (CSRF). The "caveat" is that if the app being deployed is a PUBLIC API, a wildcard "*" CORS policy is absolutely necessary.

Audit:

Audit from Azure Portal

1. Go to **App Service**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **API**, click **CORS**.
6. Ensure **Allowed Origins** does not include *****.
7. Repeat steps 1-6 for each app and deployment slot.

Audit from Azure CLI

Run the following command to list apps:

```
az webapp list
```

For each app, run the following command to list deployment slots:

```
az webapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the CORS allowed origins setting:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<app-  
name>/slots/<deployment-slot-name> --query properties.cors.allowedOrigins
```

Ensure that the response does not include *****.

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:** [cae7c12e-764b-4c87-841a-fdc6675d196f](#) - **Name:** 'App Service app slots should not have CORS configured to allow every resource to access your apps'

Remediation:

Remediate from Azure Portal

1. Go to **App Service**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **API**, click **CORS**.
6. Under **Allowed Origins**, delete the entry that equals *****.
7. Specify the origins that should be allowed to make cross-origin calls.
8. Click **Save**.
9. Repeat steps 1-8 for each app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to update the allowed origins array to contain only the origins that should be allowed:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<app-  
name>/slots/<deployment-slot-name> --set  
properties.cors.allowedOrigins="['<allowed-origin>']"
```

Default Value:





By default, CORS is not configured.

References:

1. <https://learn.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-rest-api>
2. <https://learn.microsoft.com/en-us/cli/azure/webapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

4. <https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers-Cheat-Sheet.html>
5. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CORS>
6. <https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site-Request-Forgery-Prevention-Cheat-Sheet.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>16.1 <u>Establish and Maintain a Secure Application Development Process</u></p> <p>Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v7	<p>18.1 <u>Establish Secure Coding Practices</u></p> <p>Establish secure coding practices appropriate to the programming language and development environment being used.</p>			

2.3 Function Apps

2.3.1 Ensure 'Java version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Java may be deprecated and no longer supported. Using a supported version of Java for function apps is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of currently supported versions of Java here:

<https://www.oracle.com/java/technologies/java-se-support-roadmap.html>

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, ensure that for a **Stack** of **Java**, the **Java Version** reflects a currently supported release.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the Java version:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query siteConfig.[javaContainer,javaContainerVersion,javaVersion,linuxFxVersion]
```

If Java is in use, ensure the version is currently supported.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

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

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name  
<function-app-name>
```

Run the following command to get the Java version:

```
$app.SiteConfig | Select-Object JavaContainer, JavaContainerVersion,  
JavaVersion, LinuxFXVersion, WindowsFxVersion
```

If Java is in use, ensure the version is currently supported.
Repeat for each function app.

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:** [9d0b6ea4-93e2-4578-bf2f-6bb17d22b4bc](#) - **Name:** 'Function apps that use Java should use a specified 'Java version''

Remediation:

Note: No action is required if Java is not in use.

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, for a **Stack of Java**, set the **Java Version** to a currently supported release.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az functionapp list-runtimes
```

For each function app requiring remediation, run the following command with the appropriate parameters to update the Java version:

```
az functionapp config set --resource-group <resource-group-name> --name  
<function-app-name> [--java-container <java-container> --java-container-  
version <java-container-version> --java-version <java-version>] [--linux-fx-  
version <java-runtime-version>]
```







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-language-java-deploy-run>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://www.oracle.com/java/technologies/java-se-support-roadmap.html>
5. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
6. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.3.2 Ensure 'Python version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Python may be deprecated and no longer supported. Using a supported version of Python for function apps is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions (given a status of "security") of Python here: <https://devguide.python.org/versions/>

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, ensure that for a **Stack** of **Python**, the **Python Version** reflects a currently supported release.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the Python version:

```
az functionapp config show --resource-group <resource-group-name> --name <app-name> --query "{LinuxFxVersion:linuxFxVersion,PythonVersion:pythonVersion}"
```

If Python is in use, ensure the version is currently supported.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

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

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name  
<function-app-name>
```

Run the following command to get the Python version:

```
$app.SiteConfig | Select-Object LinuxFxVersion, PythonVersion
```

If Python is in use, ensure the version is currently supported.
Repeat for each function app.

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:** [7238174a-fd10-4ef0-817e-fc820a951d73](#) - **Name:** 'Function apps that use Python should use a specified 'Python version''

Remediation:

Note: No action is required if Python is not in use.

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, for a **Stack of Python**, set the **Python Version** to a currently supported release.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az functionapp list-runtimes
```

For each function app requiring remediation, run the following command with the appropriate parameters to update the Python version:

```
az functionapp config set --resource-group <resource-group-name> --name <app-name>  
--linux-fx-version "PYTHON|<version>"
```







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#configure-language-stack-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://devguide.python.org/versions/>
5. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
6. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.3.3 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

Basic Authentication Publishing Credentials provides the ability to publish—or deploy to—a function app without a centralized Identity Provider. For a more effective, capable, and secure solution for Identity, Authentication, Authorization, and Accountability, a centralized Identity Provider such as Entra ID is strongly advised.

Rationale:

Basic Authentication introduces an identity silo for privileged access to a resource and produces logging which may not provide a full chain of accountability. This can be exploited in numerous ways and represents a significant vulnerability and attack vector.

Impact:

Disabling 'Basic Auth Publishing Credentials' will prevent the following deployment methods from working:

FTP Basic Auth Publishing Credentials:

- FTP
- FTPS

SCM Basic Auth Publishing Credentials:

- Local Git
- GitHub
- Azure Repos
- Bitbucket
- Visual Studio (Version 17.12 and earlier)

If this recommendation cannot be implemented because one of the above listed deployment methods is necessary and cannot be adapted, compensating controls (e.g. using FTPS Only and disabling only "SCM Basic Auth Publishing Credentials") are recommended to reduce potential attack surface.

An Identity Provider that can be used by the function app for authenticating users is required.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, ensure that **SCM Basic Auth Publishing Credentials** and **FTP Basic Auth Publishing Credentials** are set to **Off**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the basic authentication for FTP setting:

```
az resource show --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name> --query properties.allow
```

Ensure that **false** is returned.

For each function app, run the following command to get the basic authentication for SCM setting:

```
az resource show --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name> --query properties.allow
```

Ensure that **false** is returned.

Remediation:

CAUTION: Applying changes may cause your function app to restart.

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, set **SCM Basic Auth Publishing Credentials** and **FTP Basic Auth Publishing Credentials** to **Off**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to disable basic authentication for FTP:

```
az resource update --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name> --set properties.allow=false
```

For each function app requiring remediation, run the following command to disable basic authentication for SCM:

```
az resource update --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name> --set properties.allow=false
```





Default Value:

Basic authentication is disabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-basic-auth-disable>
2. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

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.			

2.3.4 Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

By default, App Service supports deployment over FTP. If FTP is essential for a deployment workflow, FTPS should be enforced for all function apps.

If FTPS is not explicitly required, the recommended setting is **Disabled**.

Rationale:

FTP is an unencrypted network protocol that transmits data—including passwords—in clear text. The use of this protocol can lead to both data and credential compromise and can present opportunities for exfiltration, persistence, and lateral movement.

Impact:

Deployment workflows that rely on FTP or FTPS rather than WebDeploy or HTTPS endpoints may be affected.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, ensure that **FTP state** is set to **FTPS only** or **Disabled**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the FTPS state setting:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query siteConfig.ftpState
```

Ensure that **"FtpsOnly"** or **"Disabled"** is returned.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

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

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name  
<function-app-name>
```

Run the following command to get the FTPS state setting:

```
$app.SiteConfig.FtpsState
```

Ensure that "FtpsOnly" or "Disabled" is returned.
Repeat for each function app.

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:** [399b2637-a50f-4f95-96f8-3a145476eb15](#) - **Name:** 'Function apps should require FTPS only'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, set **FTP state** to **FTPS only** or **Disabled**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to set FTPS state to **FtpsOnly** or **Disabled**:

```
az functionapp config set --resource-group <resource-group-name> --name  
<function-app-name> --ftps-state <FtpsOnly|Disabled>
```





Default Value:

By default, FTP state is set to **FTPS only**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/deploy-ftp>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-security>
3. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-how-to-use-azure-function-app-settings#https-deployment-settings>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit>
6. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
7. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>

CIS Controls:

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

2.3.5 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for HTTP, either due to security flaws or to include additional functionalities. Using the latest HTTP version allows apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.

Rationale:

Newer versions may contain security enhancements and additional functionalities. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

HTTP 2.0 has additional performance improvements for the head-of-line blocking problem of the old HTTP version, header compression, and request prioritization. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient mechanisms for data streaming.

Impact:

Most modern browsers support the HTTP/2 protocol over TLS only, while non-encrypted traffic continues to use HTTP/1.1. To ensure that client browsers connect to your app with HTTP/2, either purchase an App Service Certificate for your app's custom domain or bind a third-party certificate.

NOTE: HTTP/2 cannot be used in tandem with mutual authentication or client certificates.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, ensure that **HTTP version** is set to **2.0**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the **http20Enabled** setting:

```
az functionapp config show --resource-group <resource-group-name> --name  
<function-app-name> --query http20Enabled
```

Ensure that **true** is returned.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

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

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name  
<function-app-name>
```

Run the following command to get the **Http20Enabled** setting:

```
$app.SiteConfig.Http20Enabled
```

Ensure that **True** is returned.

Repeat for each function app.

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:** [e2c1c086-2d84-4019-bff3-c44ccd95113c](#) - **Name:** 'Function apps should use latest 'HTTP Version''

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, set **HTTP version** to **2.0**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to enable **http20Enabled**:

```
az functionapp config set --resource-group <resource-group-name> --name <app-name> --http20-enabled true
```







Default Value:

By default, **HTTP version** is set to **1.1**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#general-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>

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.			

2.3.6 Ensure 'HTTPS Only' is set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

Azure App Service allows function apps to run under both HTTP and HTTPS by default. Function apps can be accessed by anyone using non-secure HTTP links by default. Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic.

Rationale:

Enabling HTTPS-only traffic will redirect all non-secure HTTP requests to HTTPS ports. HTTPS uses the TLS/SSL protocol to provide a secure connection which is both encrypted and authenticated. It is therefore important to support HTTPS for the security benefits.

Impact:

When it is enabled, every incoming HTTP request is redirected to the HTTPS port. This means an extra level of security will be added to the HTTP requests made to the deployment slot.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** tab, under **Platform settings**, ensure that **HTTPS Only** is set to **On**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the HTTPS setting:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query "httpsOnly"
```

Ensure that the command returns **true**.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

Run the following command to get the function app with a given name:

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name  
<function-app-name>
```

Run the following command to get the HTTPS setting for the function app:

```
$app.httpsOnly
```

Ensure that the command returns **True**.

Repeat for each function app.

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:** [6d555dd1-86f2-4f1c-8ed7-5abae7c6cbab](#) - **Name:** 'Function apps should only be accessible over HTTPS'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** tab, under **Platform settings**, next to **HTTPS Only**, select the radio button next to **On**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to enable **HTTPS Only**:

```
az resource update --resource-group <resource-group-name> --name <function-  
app-name> --resource-type "Microsoft.Web/sites" --set  
properties.httpsOnly=true
```





Default Value:

HTTPS Only is enabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-security#https-and-certificates>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://techcommunity.microsoft.com/t5/azure-paas-blog/enable-https-setting-on-azure-app-service-using-azure-policy/ba-p/3286603>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>
6. <https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts>
7. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.3.7 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)

Profile Applicability:

- Level 1

Description:

The TLS (Transport Layer Security) protocol secures the transmission of data over the internet using standard encryption technology. Function apps use TLS 1.2 for the **Minimum Inbound TLS Version** by default and allow for the use of TLS versions 1.0, 1.1, and 1.3. NIST strongly suggests the use of TLS 1.2 and recommends the adoption of TLS 1.3.

Rationale:

TLS 1.0 and 1.1 are outdated and vulnerable to security risks. Since TLS 1.2 and TLS 1.3 provide enhanced security and improved performance, it is highly recommended to use TLS 1.2 or higher whenever possible.

Impact:

Using the latest TLS version may affect compatibility with clients and backend services.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, ensure that **Minimum Inbound TLS Version** is set to **1.2** or higher.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the TLS version setting:

```
az functionapp config show --resource-group <resource-group-name> --name  
<function-app-name> --query minTlsVersion
```

Ensure that **"1.2"** or higher is returned.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

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

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name  
<function-app-name>
```

Run the following command to get the TLS version setting:

```
$app.SiteConfig.MinTlsVersion
```

Ensure that the command returns **1.2** or higher.

Repeat for each function app.

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:** [f9d614c5-c173-4d56-95a7-b4437057d193](#) - **Name:** 'Function apps should use the latest TLS version'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Platform settings**, click the drop-down next to **Minimum Inbound TLS Version** and select **1.2** or higher.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to update the TLS version:

```
az functionapp config set --resource-group <resource-group-name> --name  
<function-app-name> --min-tls-version <1.2|1.3>
```





Default Value:

By default, TLS version is set to 1.2.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-bindings#how-can-i-change-the-minimum-tls-versions-for-the-app>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-8-detect-and-disable-insecure-services-and-protocols>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>
6. <https://csrc.nist.gov/news/2019/nist-publishes-sp-800-52-revision-2>

CIS Controls:

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

2.3.8 Ensure end-to-end TLS encryption is enabled (Automated)

Profile Applicability:

- Level 1

Description:

End-to-end (E2E) TLS encryption ensures that front-end to worker communication within function apps is encrypted using TLS. Without this feature, while incoming HTTPS requests are encrypted to the front ends, the traffic from front ends to workers running the application workloads would travel unencrypted inside Azure's infrastructure.

Rationale:

E2E TLS helps ensure full encryption of traffic between:

- Clients and front ends
- Front ends and worker processes hosting the application

Impact:

Enabling end-to-end TLS encryption may introduce minimal latency and require additional configuration of certificates and HTTPS settings to ensure compatibility.

Audit:

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the end-to-end TLS encryption setting:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query endToEndEncryptionEnabled
```

Ensure that the command returns **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:** [387140f1-6da9-4741-bcee-3b5edcfd9ec](#) - **Name:** 'Function apps should enable end to end encryption'

Remediation:

Remediate from Azure CLI

For each function app requiring remediation, run the following command to enable end-to-end TLS encryption:

```
az resource update --resource-group <resource-group-name> --name <function-app-name> --resource-type "Microsoft.Web/sites" --set properties.endToEndEncryptionEnabled=true
```





Default Value:

By default, end-to-end TLS encryption is disabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-tls#end-to-end-tls-encryption>
2. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.3.9 Ensure 'Remote debugging' is set to 'Off' (Automated)

Profile Applicability:

- Level 1

Description:

Remote debugging allows a function app to be debugged in real-time directly in the Azure environment. When remote debugging is enabled, it opens a communication channel that could potentially be exploited by unauthorized users if not properly secured.

Rationale:

Disabling remote debugging on a function app is primarily about enhancing security.

Remote debugging opens a communication channel that can be exploited by attackers. By disabling it, you reduce the number of potential entry points for unauthorized access.

If remote debugging is enabled without proper access controls, it can allow unauthorized users to connect to your function app, potentially leading to data breaches or malicious code execution.

During a remote debugging session, sensitive information might be exposed. Disabling remote debugging helps ensure that such data remains secure. This minimizes the use of remote access tools to reduce risk.

Impact:

You will not be able to connect to your function app from a remote location to diagnose and fix issues in real-time. You will not be able to step through code, set breakpoints, or inspect variables and the call stack while the function app is running on the server. Remote debugging is particularly useful for diagnosing issues that only occur in the production environment. Without it, you will need to rely on logs and other diagnostic tools.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Debugging**, ensure that **Remote debugging** is set to **Off**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the remote debugging setting:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query siteConfig.remoteDebuggingEnabled
```

Ensure that **false** is returned.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

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

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name <function-app-name>
```

Run the following command to get the remote debugging setting:

```
$app.SiteConfig.RemoteDebuggingEnabled
```

Ensure that **False** is returned.

Repeat for each function app.

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:** [0e60b895-3786-45da-8377-9c6b4b6ac5f9](#) - **Name:** 'Function apps should have remote debugging turned off'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Debugging**, set **Remote debugging** to **Off**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to disable remote debugging:

```
az functionapp config set --resource-group <resource-group-name> --name <function-app-name> --remote-debugging-enabled false
```





Default Value:

By default, remote debugging is set to **off**.

References:

1. <https://learn.microsoft.com/en-us/visualstudio/debugger/remote-debugging-azure-app-service>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-2-audit-and-enforce-secure-configurations>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.			
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.			

2.3.10 Ensure incoming client certificates are enabled and required (if in use) (Automated)

Profile Applicability:

- Level 2

Description:

Client certificates allow for the function app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app.

Rationale:

The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client with valid certificates can access the app.

Impact:

Utilizing and maintaining client certificates will require additional work to obtain and manage replacement and key rotation.

NOTE: This recommendation cannot be implemented if following the recommendation titled "Ensure 'HTTP Version' is set to '2.0' (if in use)." This recommendation should only be considered for scenarios where HTTP versions prior to 2.0 are required for an app, and mutual certificate authentication is desired for validating clients.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Incoming client certificates**, ensure that **Client certificate mode** is set to **Required**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the **clientCertEnabled** and **clientCertMode** settings:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query "[clientCertEnabled, clientCertMode]"
```

Ensure that **[true, "Required"]** is returned.

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:** [ab6a902f-9493-453b-928d-62c30b11b5a6](#) - **Name:** 'Function apps should have Client Certificates (Incoming client certificates) enabled'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Configuration**.
4. In the **General settings** pane, under **Incoming client certificates**, set **Client certificate mode** to **Required**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to enable and require incoming client certificates:

```
az resource update --resource-group <resource-group-name> --name <function-app-name> --resource-type "Microsoft.Web/sites" --set properties.clientCertEnabled=true --set properties.clientCertMode=Required
```







Default Value:

By default, incoming client certificates are disabled.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-authenticate-server-and-services>
2. <https://learn.microsoft.com/en-gb/azure/app-service/app-service-web-configure-tls-mutual-auth>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.3.11 Ensure 'App Service authentication' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2

Description:

App Service authentication can prevent anonymous HTTP requests from reaching an app, or authenticate those with tokens before they reach the app. If an anonymous request is received from a browser, App Service will redirect to a login page. To handle the login process, a choice from a set of identity providers can be made, or a custom authentication mechanism can be implemented.

Rationale:

By enabling authentication, every incoming HTTP request passes through it before being handled by the application code. It also handles authentication of users with the specified provider (Entra ID, Facebook, Google, Microsoft Account, and Twitter), validation, storage and refreshing of tokens, managing the authenticated sessions, and injecting identity information into request headers.

Impact:

This is only required for apps that require authentication. Enabling it on a site like a marketing or support website will prevent unauthenticated access, which would be undesirable.

Adding an authentication requirement will increase costs and require additional security components to facilitate the authentication.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Authentication**.
4. Ensure that **App Service authentication** is set to **Enabled**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the authentication setting:

For v1 auth commands:

```
az webapp auth show --resource-group <resource-group-name> --name <function-app-name> --query enabled
```

For v2 auth commands:

```
az webapp auth show --resource-group <resource-group-name> --name <function-app-name> --query properties.platform.enabled
```

Ensure that **true** is returned.

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:** [c75248c1-ea1d-4a9c-8fc9-29a6aabd5da8](#) - **Name:** 'Function apps should have authentication enabled'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Authentication**.
4. If an identity provider is not configured:
 1. Click **Add identity provider**.
 2. Provide appropriate configuration for an identity provider and click **Add**.
5. If **App Service authentication** is set to **Disabled**:
 1. Click **Enable authentication**.
6. Repeat steps 1-5 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to enable authentication:

```
az webapp auth update --resource-group <resource-group-name> --name <function-app-name> --enabled true
```

Note: In order to access **App Service authentication** settings for an app using the Microsoft API, the **Website Contributor** permission at the subscription level is required. A custom role can be created instead of **Website Contributor** to provide more specific permissions and maintain the principle of least privileged access.

Default Value:

By default, **App Service authentication** is set to **Disabled**.







References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>
2. <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#website-contributor>
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-6-define-and-implement-identity-and-privileged-access-strategy>
5. <https://learn.microsoft.com/en-us/cli/azure/webapp/auth>

Additional Information:

You're not required to use App Service for authentication and authorization. Many web frameworks come with security features built in, and you can use them if you like. If you need more flexibility than App Service provides, you can also write your own utilities. Secure authentication and authorization require a deep understanding of security, including federation, encryption, JSON Web Token (JWT) management, grant types, and so on.

CIS Controls:

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

2.3.12 Ensure managed identities are configured (Automated)

Profile Applicability:

- Level 1

Description:

Managed identities from Microsoft Entra ID allow function apps to securely access other Azure services without the need to provision or rotate any secrets.

Rationale:

Using managed identities with function apps eliminates the need to store and manage credentials to access Azure resources.

Impact:

Minor administrative overhead to configure and manage role assignments for managed identities.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Identity**.
4. Ensure that in the **System assigned** pane, the **Status** is set to **On**, and an **Object (principal) ID** is displayed, or that in the **User assigned** pane, a managed identity is listed.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the identity setting:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query "identity"
```

Ensure that **type** is set to **SystemAssigned**, **UserAssigned**, or both.

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:** [0da106f2-4ca3-48e8-bc85-c638fe6aea8f](#) - **Name:** 'Function apps should use managed identity'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Identity**.
4. To add a system assigned managed identity:
 1. In the **System assigned** pane, under **Status**, click **On**.
 2. Click **Save**.
 3. Click **Yes**.
5. To add a user assigned managed identity:
 1. In the **User assigned** pane, click **Add**.
 2. Use the filter box to search for a managed identity.
 3. Select the identity.
 4. Click **Add**.
6. Repeat steps 1-5 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to assign a system-assigned managed identity:

```
az functionapp identity assign --resource-group <resource-group-name> --name <function-app-name>
```

Remediate from PowerShell

For each function app requiring remediation, run the following command to assign a system-assigned managed identity:

```
Update-AzFunctionApp -ResourceGroupName <resource-group-name> -Name <function-app-name> -IdentityType SystemAssigned -Force
```





Default Value:

Managed identities are disabled by default for function apps.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-1-use-centralized-identity-and-authentication-system>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.functions/update-azfunctionapp>

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.			

2.3.13 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 the service is not directly exposed to the public Internet. This has the added benefit of providing more granular control over security settings and configurations for those additional layers of separation.

Impact:

NOTE: Prior to disabling public network access, it is strongly recommended that, for each function app, either:

- complete virtual network integration as described in **"Ensure app is integrated with a virtual network"**

OR

- set up private endpoints/links as described in **"Ensure private endpoints are used to access App Service apps."**

Disabling public network access restricts direct access to the service. This enhances security but will require the configuration of a virtual network and/or private endpoints for any services or users needing access within trusted networks.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Networking**.
4. Under **Inbound traffic configuration**, ensure that **Public network access** is set to **Disabled**.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the public network access setting:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query "publicNetworkAccess"
```

Ensure that the command returns **"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:** [969ac98b-88a8-449f-883c-2e9adb123127](#) - **Name:** 'Function apps should disable public network access'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Networking**.
4. Under **Inbound traffic configuration**, click the text next to **Public network access**.
5. Select the radio button next to **Disabled**.
6. Click **Save**.
7. Check the box to confirm the change.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to disable public network access:

```
az resource update --resource-group <resource-group-name> --name <function-app-name> --resource-type "Microsoft.Web/sites" --set properties.publicNetworkAccess=Disabled
```







Default Value:

By default, public network access is enabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/networking-features>
2. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.3.14 Ensure function app is integrated with a virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Integrate function apps with a virtual network to enable access to resources in or through a non-internet-routable virtual network.

This recommendation does not apply to function apps created on the consumption hosting plan, which does not support virtual networking.

Rationale:

Integrate function apps with a virtual network for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, ensure that a virtual network and subnet name are displayed.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the virtual network subnet ID:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query "virtualNetworkSubnetId"
```

Ensure that a virtual network subnet ID is returned.

Audit from PowerShell

Run the following command to list function apps:

```
Get-AzFunctionApp
```

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

```
$app = Get-AzFunctionApp -ResourceGroupName <resource-group-name> -Name  
<function-app-name>
```

Run the following command to get the virtual network subnet ID:

```
$app.virtualNetworkSubnetId
```

Ensure that a virtual network subnet ID is returned.
Repeat for each function app.

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, click **Not configured**.
5. Click **Add virtual network integration**.
6. Select an existing App Service Plan connection, or select **New connection** and select a subscription, virtual network, and subnet.
7. Click **Connect**.
8. Repeat steps 1-7 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to integrate with a virtual network:

```
az functionapp vnet-integration add --resource-group <resource-group-name> --  
name <function-app-name> --vnet <virtual-network-name> --subnet <subnet-name>
```

Remediate from PowerShell

For each function app requiring remediation, run the following commands to integrate with a virtual network:

Prepare parameters:

```
$siteName = '<app-name>'  
$vNetResourceGroupName = '<virtual-network-resource-group-name>'  
$functionAppResourceGroupName = '<function-app-resource-group-name>'  
$vNetName = '<virtual-network-name>'  
$integrationSubnetName = '<subnet-name>'  
$vNetSubscriptionId = '<subscription-guid>'
```

Check if the subnet is delegated to **Microsoft.Web/serverFarms**:

```
$vnet = Get-AzVirtualNetwork -Name $vNetName -ResourceGroupName  
$vNetResourceGroupName  
$subnet = Get-AzVirtualNetworkSubnetConfig -Name $integrationSubnetName -  
VirtualNetwork $vnet  
Get-AzDelegation -Subnet $subnet
```

Add delegation:

```
$subnet = Add-AzDelegation -Name "myDelegation" -ServiceName  
"Microsoft.Web/serverFarms" -Subnet $subnet  
Set-AzVirtualNetwork -VirtualNetwork $vnet
```

Configure virtual network integration:

```
$subnetResourceId =  
"/subscriptions/$vNetSubscriptionId/resourceGroups/$vNetResourceGroupName/pro  
viders/Microsoft.Network/virtualNetworks/$vNetName/subnets/$integrationSubnet  
Name"  
$functionApp = Get-AzResource -ResourceType Microsoft.Web/sites -  
ResourceGroupName $functionAppResourceGroupName -ResourceName $siteName  
$functionApp.Properties.virtualNetworkSubnetId = $subnetResourceId  
$functionApp.Properties.vnetRouteAllEnabled = 'true'  
$functionApp | Set-AzResource -Force
```





Default Value:

By default, virtual network integration is not configured.

References:

1. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-networking-options>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>
3. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-enable>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/powershell/module/az.functions/get-azfunctionapp>

CIS Controls:

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

2.3.15 Ensure configuration is routed through the virtual network integration (Automated)

Profile Applicability:

- Level 2

Description:

By default, configuration traffic for function apps goes directly over the public route. Container image pulls and content sharing can be routed through the virtual network integration.

This recommendation should be applied after integrating a function app with a virtual network.

Rationale:

Route container image pulls and content sharing through a virtual network integration for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the container image share and content share settings:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query "[vnetImagePullEnabled,vnetContentShareEnabled]"
```

Ensure that **[true,true]** is returned.

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:** [5e57f5ad-995a-485b-9f42-4748935ee5d9](#) - **Name:** 'Function apps should enable configuration routing to Azure Virtual Network'

Remediation:

Remediate from Azure CLI

For each function app requiring remediation, run the following command to route container image pulls and content sharing through the virtual network integration:

```
az resource update --resource-group <resource-group-name> --name <function-app-name> --resource-type "Microsoft.Web/sites" --set properties.vnetImagePullEnabled=true --set properties.vnetContentShareEnabled=true
```

Default Value:

By default, configuration traffic goes directly over the public route.





References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#routes>
2. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-configuration-routing>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

Additional Information:

In addition to configuring the routing for content sharing, you must also ensure that any firewall or Network Security Group configured on traffic from the subnet allow traffic to port 443 and 445.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 <u>Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3.16 Ensure all traffic is routed through the virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Enable `vnetRouteAllEnabled` to ensure all outbound traffic is routed through the integrated virtual network.

This recommendation should be applied after integrating a function app with a virtual network.

Rationale:

Routing all outbound traffic through the virtual network enhances security.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
5. Under **Application routing**, ensure that the box next to **Outbound internet traffic** is checked.
6. Repeat steps 1-5 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the virtual network traffic routing setting:

```
az functionapp show --resource-group <resource-group-name> --name <app-name> --query vnetRouteAllEnabled
```

Ensure that `true` is returned.

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:** [32a913ec-5ed7-4b31-a5b0-198450d8fb13](#) - **Name:** 'Function apps should enable outbound non-RFC 1918 traffic to Azure Virtual Network'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Settings**, click **Networking**.
4. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
5. Under **Application routing**, check the box next to **Outbound internet traffic**.
6. Click **Apply**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command to route all traffic through the virtual network:

```
az resource update --resource-group <resource-group-name> --name <function-app-name> --resource-type "Microsoft.Web/sites" --set properties.vnetRouteAllEnabled=true
```





Default Value:

For function apps integrated with a virtual network, all traffic is routed through the virtual network by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-application-routing>
2. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-app-settings#vnetrouteallenabled>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>13.4 Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3.17 Ensure cross-origin resource sharing does not allow all origins (Automated)

Profile Applicability:

- Level 2

Description:

Cross-origin resource sharing (CORS) is a security feature that controls how applications interact with resources hosted on different domains.

Rationale:

Restrict CORS to only trusted origins to help enforce proper access control and reduce exposure to malicious cross-origin requests.

Impact:

Configuration is required to ensure that the appropriate origins have access.

Setting up a proper CORS policy can be fairly complex and an incorrect setting could permit Cross-Site Request Forgery (CSRF). The "caveat" is that if the app being deployed is a PUBLIC API, a wildcard "*" CORS policy is absolutely necessary.

Audit:

Audit from Azure Portal

1. Go to **App Service** or **Function App**.
2. Click the name of a function app.
3. Under **API**, click **CORS**.
4. Ensure **Allowed Origins** does not include *****.
5. Repeat steps 1-4 for each function app.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to get the CORS allowed origins setting:

```
az functionapp show --resource-group <resource-group-name> --name <function-app-name> --query siteConfig.cors.allowedOrigins
```

Ensure that the response does not include *****.

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:** [0820b7b9-23aa-4725-a1ce-ae4558f718e5](#) - **Name:** 'Function apps should not have CORS configured to allow every resource to access your apps'

Remediation:

Remediate from Azure Portal

1. Go to **App Service** or **Function App**.
2. Click the name of a function app.
3. Under **API**, click **CORS**.
4. Under **Allowed Origins**, delete the entry that equals *****.
5. Specify the origins that should be allowed to make cross-origin calls.
6. Click **Save**.
7. Repeat steps 1-6 for each function app requiring remediation.

Remediate from Azure CLI

For each function app requiring remediation, run the following command:

```
az functionapp cors remove --resource-group <resource-group-name> --name  
<function-app-name> --allowed-origins ""
```

Use the following command to specify the origins that should be allowed:

```
az functionapp cors add --resource-group <resource-group-name> --name  
<function-app-name> --allowed-origins <allowed-origins>
```





Default Value:

By default, **Allowed Origins** is set to <https://portal.azure.com>.

References:

1. <https://learn.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-rest-api>
2. <https://learn.microsoft.com/en-us/cli/azure/functionapp/cors>
3. <https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers-Cheat-Sheet.html>
4. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CORS>
5. <https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site-Request-Forgery-Prevention-Cheat-Sheet.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.1 <u>Establish and Maintain a Secure Application Development Process</u> Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	18.1 <u>Establish Secure Coding Practices</u> Establish secure coding practices appropriate to the programming language and development environment being used.			

2.4 Functions Deployment Slots

2.4.1 Ensure 'Java version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Java may be deprecated and no longer supported. Using a supported version of Java for function app deployment slots is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of currently supported versions of Java here:

<https://www.oracle.com/java/technologies/java-se-support-roadmap.html>

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, ensure that for a **Stack** of **Java**, the **Java Version** reflects a currently supported release.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, run the following command to get the Java version:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --query  
properties.[javaContainer,javaContainerVersion,javaVersion,linuxFxVersion]
```

If Java is in use, ensure the version is currently supported.

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:** [e1d1b522-02b0-4d18-a04f-5ab62d20445f](#) - **Name:** 'Function app slots that use Java should use a specified 'Java version''

Remediation:

Note: No action is required if Java is not in use.

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, for a **Stack of Java**, set the **Java Version** to a currently supported release.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az functionapp list-runtimes
```

For each deployment slot requiring remediation, run the following command with the appropriate parameters to update the Java version:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --set  
properties.[javaContainer|javaContainerVersion|javaVersion|linuxFxVersion]="<  
java-container|java-container-version|java-version|java-runtime-version>"
```







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-language-java-deploy-run>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://www.oracle.com/java/technologies/java-se-support-roadmap.html>
5. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
6. <https://learn.microsoft.com/en-us/cli/azure/resource>

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.			

2.4.2 Ensure 'Python version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Python may be deprecated and no longer supported. Using a supported version of Python for function app deployment slots is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions (given a status of "security") of Python here: <https://devguide.python.org/versions/>

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, ensure that for a **Stack** of **Python**, the **Python Version** reflects a currently supported release.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, run the following command to get the Python version:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --query  
properties.[linuxFxVersion,pythonVersion]
```

If Python is in use, ensure the version is currently supported.

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:** [829b40f3-d3db-4fd2-be46-76663d3aeeb2](#) - **Name:** 'Function app slots that use Python should use a specified 'Python version''

Remediation:

Note: No action is required if Python is not in use.

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, for a **Stack** of **Python**, set the **Python Version** to a currently supported release.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

Run the following command to list supported runtimes:

```
az functionapp list-runtimes
```

For each deployment slot requiring remediation, run the following command with the appropriate parameters to update the Python version:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --set  
properties.linuxFxVersion="PYTHON|<python-version>"
```







Default Value:

The version is selected during creation.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#configure-language-stack-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://devguide.python.org/versions/>
5. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
6. <https://learn.microsoft.com/en-us/cli/azure/resource>

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.			

2.4.3 Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

Basic Authentication Publishing Credentials provides the ability to publish—or deploy to—a function app deployment slot without a centralized Identity Provider. For a more effective, capable, and secure solution for Identity, Authentication, Authorization, and Accountability, a centralized Identity Provider such as Entra ID is strongly advised.

This recommendation applies to function apps using the Consumption, Premium, or Dedicated (App Service) plans, which support deployment slots.

Rationale:

Basic Authentication introduces an identity silo for privileged access to a resource and produces logging which may not provide a full chain of accountability. This can be exploited in numerous ways and represents a significant vulnerability and attack vector.

Impact:

Disabling 'Basic Auth Publishing Credentials' will prevent the following deployment methods from working:

FTP Basic Auth Publishing Credentials:

- FTP
- FTPS

SCM Basic Auth Publishing Credentials:

- Local Git
- GitHub
- Azure Repos
- Bitbucket
- Visual Studio (Version 17.12 and earlier)

If this recommendation cannot be implemented because one of the above listed deployment methods is necessary and cannot be adapted, compensating controls (e.g. using FTPS Only and disabling only "SCM Basic Auth Publishing Credentials") are recommended to reduce potential attack surface.

An Identity Provider that can be used by the function app deployment slot for authenticating users is required.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of an app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **SCM Basic Auth Publishing Credentials** and **FTP Basic Auth Publishing Credentials** are set to **Off**.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, run the following command to get the basic authentication for FTP setting:

```
az resource show --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name>/slots/<deployment-slot-name> --query properties.allow
```

Ensure that **false** is returned.

For each deployment slot, run the following command to get the basic authentication for SCM setting:

```
az resource show --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name>/slots/<deployment-slot-name> --query properties.allow
```

Ensure that **false** is returned.

Remediation:

CAUTION: Applying changes may cause your App Service resource to restart.

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.

5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, set **SCM Basic Auth Publishing Credentials** and **FTP Basic Auth Publishing Credentials** to **Off**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to disable basic authentication for FTP:

```
az resource update --resource-group <resource-group-name> --name ftp --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name>/slots/<deployment-slot-name> --set properties.allow=false
```

For each deployment slot requiring remediation, run the following command to disable basic authentication for SCM:

```
az resource update --resource-group <resource-group-name> --name scm --namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --parent sites/<function-app-name>/slots/<deployment-slot-name> --set properties.allow=false
```





Default Value:

Basic authentication is enabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-basic-auth-disable>
2. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

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.			

2.4.4 Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

By default, App Service supports deployment over FTP. If FTP is essential for a deployment workflow, FTPS should be enforced for all function app deployment slots.

If FTPS is not explicitly required, the recommended setting is **Disabled**.

Rationale:

FTP is an unencrypted network protocol that transmits data—including passwords—in clear text. The use of this protocol can lead to both data and credential compromise and can present opportunities for exfiltration, persistence, and lateral movement.

Impact:

Deployment workflows that rely on FTP or FTPS rather than WebDeploy or HTTPS endpoints may be affected.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment Slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **FTP state** is set to **FTPS only** or **Disabled**.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, run the following command to get the FTPS state setting:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --query properties.ftpState
```

Ensure that "FtpsOnly" or "Disabled" is returned.

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:** [e1a09430-221d-4d4c-a337-1edb5a1fa9bb](#) - **Name:** 'Function app slots should require FTPS only'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment Slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, set **FTP state** to **FTPS only** or **Disabled**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to set FTPS state to **FtpsOnly** or **Disabled**:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --set  
properties.ftpState=<FtpsOnly|Disabled>
```





Default Value:

By default, FTP state is set to **FTPS only**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/deploy-ftp>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-security>
3. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-how-to-use-azure-function-app-settings#https-deployment-settings>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/cli/azure/resource>
6. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit>
7. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>

CIS Controls:

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

2.4.5 Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for HTTP, either due to security flaws or to include additional functionalities. Using the latest HTTP version allows apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.

Rationale:

Newer versions may contain security enhancements and additional functionalities. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

HTTP 2.0 has additional performance improvements for the head-of-line blocking problem of the old HTTP version, header compression, and request prioritization. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient mechanisms for data streaming.

Impact:

Most modern browsers support the HTTP/2 protocol over TLS only, while non-encrypted traffic continues to use HTTP/1.1. To ensure that client browsers connect to your app with HTTP/2, either purchase an App Service Certificate for your app's custom domain or bind a third-party certificate.

NOTE: HTTP/2 cannot be used in tandem with mutual authentication or client certificates.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **HTTP version** is set to **2.0**.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the **http20Enabled** setting:

```
az resource show --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<function-app-name>/slots/<deployment-slot-name> --query properties.http20Enabled
```

Ensure that **true** is returned.

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:** [fa98f1b1-1f56-4179-9faf-93ad82f3458f](#) - **Name:** 'Function app slots should use latest 'HTTP Version''

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, set **HTTP version** to **2.0**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable **http20Enabled**:

```
az resource update --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<app-name>/slots/<deployment-slot-name> --set properties.http20Enabled=true
```







Default Value:

By default, **HTTP version** is set to **1.1**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-common#general-settings>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.4.6 Ensure 'HTTPS Only' is set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

Azure App Service allows function app deployment slots to run under both HTTP and HTTPS by default. Function app deployment slots can be accessed by anyone using non-secure HTTP links by default. Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic.

This recommendation applies to function apps using the Consumption, Premium, or Dedicated (App Service) plans, which support deployment slots.

Rationale:

Enabling HTTPS-only traffic will redirect all non-secure HTTP requests to HTTPS ports. HTTPS uses the TLS/SSL protocol to provide a secure connection which is both encrypted and authenticated. It is therefore important to support HTTPS for the security benefits.

Impact:

When it is enabled, every incoming HTTP request is redirected to the HTTPS port. This means an extra level of security will be added to the HTTP requests made to the deployment slot.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** tab, under **Platform settings**, ensure that **HTTPS Only** is set to **On**.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that **httpsOnly** 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:** [5e5dbe3f-2702-4ffc-8b1e-0cae008a5c71](#) - **Name:** 'Function app slots should only be accessible over HTTPS'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** tab, under **Platform settings**, next to **HTTPS Only**, select the radio button next to **On**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable **HTTPS Only**:

```
az resource update --resource-group <resource-group-name> --name <function-app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.httpsOnly=true
```





Default Value:

HTTPS Only is enabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-security#https-and-certificates>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://techcommunity.microsoft.com/t5/azure-paas-blog/enable-https-setting-on-azure-app-service-using-azure-policy/ba-p/3286603>
4. <https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts>
5. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-deployment-slots>
6. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
7. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.4.7 Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)

Profile Applicability:

- Level 1

Description:

The TLS (Transport Layer Security) protocol secures the transmission of data over the internet using standard encryption technology. Function app deployment slots use TLS 1.2 for the **Minimum Inbound TLS Version** by default and allow for the use of TLS versions 1.0, 1.1, and 1.3. NIST strongly suggests the use of TLS 1.2 and recommends the adoption of TLS 1.3.

Rationale:

TLS 1.0 and 1.1 are outdated and vulnerable to security risks. Since TLS 1.2 and TLS 1.3 provide enhanced security and improved performance, it is highly recommended to use TLS 1.2 or higher whenever possible.

Impact:

Using the latest TLS version may affect compatibility with clients and backend services.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, ensure that **Minimum Inbound TLS Version** is set to **1.2** or higher.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <app-name>
```

For each deployment slot, run the following command to get the TLS version setting:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --query properties.minTlsVersion
```

Ensure that "1.2" or higher is returned.

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:** [deb528de-8f89-4101-881c-595899253102](#) - **Name:** 'Function app slots should use the latest TLS version'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Platform settings**, click the drop-down next to **Minimum Inbound TLS Version** and select **1.2** or higher.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to update the TLS version:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --set properties.minTlsVersion=<1.2|1.3>
```

Default Value:





By default, TLS version is set to 1.2.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-ssl-bindings#how-can-i-change-the-minimum-tls-versions-for-the-app>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit>

3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-8-detect-and-disable-insecure-services-and-protocols>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
5. <https://learn.microsoft.com/en-us/cli/azure/resource>
6. <https://csrc.nist.gov/news/2019/nist-publishes-sp-800-52-revision-2>

CIS Controls:

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

2.4.8 Ensure end-to-end TLS encryption is enabled (Automated)

Profile Applicability:

- Level 1

Description:

End-to-end (E2E) TLS encryption ensures that front-end to worker communication within function app deployment slots is encrypted using TLS. Without this feature, while incoming HTTPS requests are encrypted to the front ends, the traffic from front ends to workers running the application workloads would travel unencrypted inside Azure's infrastructure.

This recommendation applies to function apps using the Consumption, Premium, or Dedicated (App Service) plans, which support deployment slots.

Rationale:

E2E TLS helps ensure full encryption of traffic between:

- Clients and front ends
- Front ends and worker processes hosting the application

Impact:

Enabling end-to-end TLS encryption may introduce minimal latency and require additional configuration of certificates and HTTPS settings to ensure compatibility.

Audit:

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that **endToEndEncryptionEnabled** 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:** [cbe0e5eb-fea9-491d-ab20-a62cf049c5ae](#) - **Name:** 'Function app slots should enable end to end encryption'

Remediation:

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable end-to-end TLS encryption:

```
az resource update --resource-group <resource-group-name> --name <function-app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.endToEndEncryptionEnabled=true
```





Default Value:

By default, end-to-end TLS encryption is disabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-tls#end-to-end-tls-encryption>
2. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
3. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.4.9 Ensure 'Remote debugging' is set to 'Off' (Automated)

Profile Applicability:

- Level 1

Description:

Remote debugging allows a function app deployment slot to be debugged in real-time directly in the Azure environment. When remote debugging is enabled, it opens a communication channel that could potentially be exploited by unauthorized users if not properly secured.

Rationale:

Disabling remote debugging on a function app deployment slot is primarily about enhancing security.

Remote debugging opens a communication channel that can be exploited by attackers. By disabling it, you reduce the number of potential entry points for unauthorized access.

If remote debugging is enabled without proper access controls, it can allow unauthorized users to connect to your deployment slot, potentially leading to data breaches or malicious code execution.

During a remote debugging session, sensitive information might be exposed. Disabling remote debugging helps ensure that such data remains secure. This minimizes the use of remote access tools to reduce risk.

Impact:

You will not be able to connect to your deployment slot from a remote location to diagnose and fix issues in real-time. You will not be able to step through code, set breakpoints, or inspect variables and the call stack while the deployment slot is running on the server. Remote debugging is particularly useful for diagnosing issues that only occur in the production environment. Without it, you will need to rely on logs and other diagnostic tools.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Debugging**, ensure that **Remote debugging** is set to **Off**.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, run the following command to get the remote debugging setting:

```
az resource show --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<function-app-name>/slots/<deployment-slot-name> --query properties.remoteDebuggingEnabled
```

Ensure that **false** is returned.

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:** [89691ef9-8c50-49a8-8950-9c7fba41699e](#) - **Name:** 'Function app slots should have remote debugging turned off'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Debugging**, set **Remote debugging** to **Off**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to disable remote debugging:

```
az resource update --name web --resource-group <resource-group-name> --namespace Microsoft.Web --resource-type config --parent sites/<function-app-name>/slots/<deployment-slot-name> --set properties.remoteDebuggingEnabled=false
```





Default Value:

By default, remote debugging is set to **off**.

References:

1. <https://learn.microsoft.com/en-us/visualstudio/debugger/remote-debugging-azure-app-service>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-2-audit-and-enforce-secure-configurations>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.			
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.			

2.4.10 Ensure incoming client certificates are enabled and required (if in use) (Automated)

Profile Applicability:

- Level 2

Description:

Client certificates allow for the deployment slot to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the deployment slot.

This recommendation applies to function apps using the Consumption, Premium, or Dedicated (App Service) plans, which support deployment slots.

Rationale:

The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client with valid certificates can access the deployment slot.

Impact:

Utilizing and maintaining client certificates will require additional work to obtain and manage replacement and key rotation.

NOTE: This recommendation cannot be implemented if following the recommendation titled "Ensure 'HTTP version' is set to '2.0' (if in use)." This recommendation should only be considered for scenarios where HTTP versions prior to 2.0 are required for a deployment slot, and mutual certificate authentication is desired for validating clients.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Incoming client certificates**, ensure that **Client certificate mode** is set to **Required**.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that **clientCertEnabled** is set to **true**, and **clientCertMode** is set to **Required**.

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:** [153ab4ca-2d58-4b5d-9134-6d8c6bdd321c](#) - **Name:** 'Function app slots should have Client Certificates (Incoming client certificates) enabled'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Configuration**.
6. In the **General settings** pane, under **Incoming client certificates**, set **Client certificate mode** to **Required**.
7. Click **Save**.
8. Click **Continue**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to enable and require incoming client certificates:

```
az resource update --resource-group <resource-group-name> --name <function-app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.clientCertEnabled=true --set properties.clientCertMode=Required
```







Default Value:

By default, incoming client certificates are disabled.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-authenticate-server-and-services>
2. <https://learn.microsoft.com/en-gb/azure/app-service/app-service-web-configure-tls-mutual-auth>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.4.11 Ensure managed identities are configured (Automated)

Profile Applicability:

- Level 1

Description:

Managed identities from Microsoft Entra ID allow function app deployment slots to securely access other Azure services without the need to provision or rotate any secrets.

This recommendation applies to function apps using the Consumption, Premium, or Dedicated (App Service) plans, which support deployment slots.

Rationale:

Using managed identities with function app deployment slots eliminates the need to store and manage credentials to access Azure resources.

Impact:

Minor administrative overhead to configure and manage role assignments for managed identities.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Identity**.
6. Ensure that in the **System assigned** pane, the **Status** is set to **On**, and an **Object (principal) ID** is displayed, or that in the **User assigned** pane, a managed identity is listed.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that **identity** contains **type** set to **SystemAssigned**, **UserAssigned**, or both.

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Identity**.
6. To add a system assigned managed identity:
 1. In the **System assigned** pane, under **Status**, click **On**.
 2. Click **Save**.
 3. Click **Yes**.
7. To add a user assigned managed identity:
 1. In the **User assigned** pane, click **Add**.
 2. Use the filter box to search for a managed identity.
 3. Select the identity.
 4. Click **Add**.
8. Repeat steps 1-7 for each function app and deployment slot requiring remediation.

Remediate from PowerShell

For each deployment slot requiring remediation, run the following command to assign a system-assigned managed identity:

```
Set-AzWebAppSlot -ResourceGroupName <resource-group-name> -Name <function-app-name> -Slot <deployment-slot-name> -AssignIdentity $true
```



Default Value:



Managed identities are disabled by default for function app deployment slots.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-1-use-centralized-identity-and-authentication-system>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebappslot>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 <u>Centralize Account Management</u> Centralize account management through a directory or identity service.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

2.4.12 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.

This recommendation applies to function apps using the Consumption, Premium, or Dedicated (App Service) plans, which support deployment slots.

Rationale:

Disabling public network access improves security by ensuring that the service is not directly exposed to the public Internet. This has the added benefit of providing more granular control over security settings and configurations for those additional layers of separation.

Impact:

NOTE: Prior to disabling public network access, it is strongly recommended that, for each function app deployment slot, either:

- complete virtual network integration as described in **"Ensure app is integrated with a virtual network"**

OR

- set up private endpoints/links as described in **"Ensure private endpoints are used to access App Service apps."**

Disabling public network access restricts direct access to the service. This enhances security but will require the configuration of a virtual network and/or private endpoints for any services or users needing access within trusted networks.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Inbound traffic configuration**, ensure that **Public network access** is set to **Disabled**.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that **publicNetworkAccess** 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:** [11c82d0c-db9f-4d7b-97c5-f3f9aa957da2](#) - **Name:** 'Function app slots should disable public network access'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Inbound traffic configuration**, click the text next to **Public network access**.
7. Select the radio button next to **Disabled**.
8. Click **Save**.
9. Check the box to confirm the change.
10. Click **Continue**.
11. Repeat steps 1-10 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to disable public network access:

```
az resource update --resource-group <resource-group-name> --name <function-app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.publicNetworkAccess=Disabled
```







Default Value:

By default, public network access is enabled.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/networking-features>
2. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-deployment-slots>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

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

2.4.13 Ensure deployment slot is integrated with a virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Integrate function app deployment slots with a virtual network to enable access to resources in or through a non-internet-routable virtual network.

This recommendation applies to function apps using the Premium or Dedicated (App Service) plans, which support deployment slots and virtual networking.

Rationale:

Integrate function app deployment slots with a virtual network for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, ensure that a virtual network and subnet name are displayed.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that **virtualNetworkSubnetId** is set to a virtual network subnet ID.

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, click **Not configured**.
7. Click **Add virtual network integration**.
8. Select an existing App Service Plan connection, or select **New connection** and select a subscription, virtual network, and subnet.
9. Click **Connect**.
10. Repeat steps 1-9 for each function app and deployment slot requiring remediation.





Default Value:

By default, virtual network integration is not configured.

References:

1. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-networking-options>
2. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration>
3. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-enable>
4. <https://learn.microsoft.com/en-us/cli/azure/functionapp>

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).			

2.4.14 Ensure configuration is routed through the virtual network integration (Automated)

Profile Applicability:

- Level 2

Description:

By default, configuration traffic for function app deployment slots goes directly over the public route. Container image pulls and content sharing can be routed through the virtual network integration.

This recommendation applies to function apps using the Premium or Dedicated (App Service) plans, which support deployment slots and virtual networking.

This recommendation should be applied after integrating a function app deployment slot with a virtual network.

Rationale:

Route container image pulls and content sharing through a virtual network integration for increased security and control.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that **vnetImagePullEnabled** and **vnetContentShareEnabled** are 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:** [f380edf5-de79-4862-bd57-ee407d8bd8b6](#) - **Name:** 'Function app slots should enable configuration routing to Azure Virtual Network'

Remediation:

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to route container image pulls and content sharing through the virtual network integration:

```
az resource update --resource-group <resource-group-name> --name <function-app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.vnetImagePullEnabled=true --set properties.vnetContentShareEnabled=true
```

Default Value:

By default, configuration traffic goes directly over the public route.





References:

1. <https://learn.microsoft.com/en-us/azure/app-service/overview-vnet-integration#routes>
2. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-configuration-routing>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

Additional Information:

In addition to configuring the routing for content sharing, you must also ensure that any firewall or Network Security Group configured on traffic from the subnet allow traffic to port 443 and 445.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 <u>Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.4.15 Ensure all traffic is routed through the virtual network (Automated)

Profile Applicability:

- Level 1

Description:

Enable `vnetRouteAllEnabled` to ensure all outbound traffic is routed through the integrated virtual network.

This recommendation should be applied after integrating a function app deployment slot with a virtual network.

Rationale:

Routing all outbound traffic through the virtual network enhances security.

Impact:

Additional configuration may be required to ensure that traffic is routed properly.

Audit:

Audit from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
7. Under **Application routing**, ensure that the box next to **Outbound internet traffic** is checked.
8. Repeat steps 1-7 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, ensure that `vnetRouteAllEnabled` 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:** [75c42c42-dfb3-453d-8fd5-9f978e1b1106](#) - **Name:** 'Function app slots should enable outbound non-RFC 1918 traffic to Azure Virtual Network'

Remediation:

Remediate from Azure Portal

1. Go to **App Services** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of a deployment slot.
5. Under **Settings**, click **Networking**.
6. Under **Outbound traffic configuration**, next to **Virtual network integration**, click the virtual network and subnet name.
7. Under **Application routing**, check the box next to **Outbound internet traffic**.
8. Click **Apply**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to route all traffic through the virtual network:

```
az resource update --resource-group <resource-group-name> --name <function-app-name>/slots/<deployment-slot-name> --resource-type "Microsoft.Web/sites" --set properties.vnetRouteAllEnabled=true
```





Default Value:

For deployment slots integrated with a virtual network, all traffic is routed through the virtual network by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/configure-vnet-integration-routing#configure-application-routing>
2. <https://learn.microsoft.com/en-us/azure/azure-functions/functions-app-settings#vnetrouteallenabled>
3. <https://learn.microsoft.com/en-us/cli/azure/functionapp>
4. <https://learn.microsoft.com/en-us/cli/azure/resource>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>13.4 Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.4.16 Ensure cross-origin resource sharing does not allow all origins (Automated)

Profile Applicability:

- Level 2

Description:

Cross-origin resource sharing (CORS) is a security feature that controls how applications interact with resources hosted on different domains.

This recommendation applies to function apps using the Consumption, Premium, or Dedicated (App Service) plans, which support deployment slots.

Rationale:

Restrict CORS to only trusted origins to help enforce proper access control and reduce exposure to malicious cross-origin requests.

Impact:

Configuration is required to ensure that the appropriate origins have access.

Setting up a proper CORS policy can be fairly complex and an incorrect setting could permit Cross-Site Request Forgery (CSRF). The "caveat" is that if the app being deployed is a PUBLIC API, a wildcard "*" CORS policy is absolutely necessary.

Audit:

Audit from Azure Portal

1. Go to **App Service** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of deployment slot.
5. Under **API**, click **CORS**.
6. Ensure **Allowed Origins** does not include *****.
7. Repeat steps 1-6 for each function app and deployment slot.

Audit from Azure CLI

Run the following command to list function apps:

```
az functionapp list
```

For each function app, run the following command to list deployment slots:

```
az functionapp deployment slot list --resource-group <resource-group-name> --name <function-app-name>
```

For each deployment slot, run the following command to get the CORS allowed origins setting:

```
az resource show --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --query properties.cors.allowedOrigins
```

Ensure that the response does not include *****.

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:** [a1a22235-dd10-4062-bd55-7d62778f41b0](#) - **Name:** 'Function app slots should not have CORS configured to allow every resource to access your apps'

Remediation:

Remediate from Azure Portal

1. Go to **App Service** or **Function App**.
2. Click the name of a function app.
3. Under **Deployment**, click **Deployment slots**.
4. Click the name of deployment slot.
5. Under **API**, click **CORS**.
6. Under **Allowed Origins**, delete the entry that equals *****.
7. Specify the origins that should be allowed to make cross-origin calls.
8. Click **Save**.
9. Repeat steps 1-8 for each function app and deployment slot requiring remediation.

Remediate from Azure CLI

For each deployment slot requiring remediation, run the following command to update the allowed origins array to contain only the origins that should be allowed:

```
az resource update --name web --resource-group <resource-group-name> --  
namespace Microsoft.Web --resource-type config --parent sites/<function-app-  
name>/slots/<deployment-slot-name> --set  
properties.cors.allowedOrigins="['<allowed-origin>']"
```

Default Value:





By default, **Allowed Origins** is set to <https://portal.azure.com>.

References:

1. <https://learn.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-rest-api>
2. <https://learn.microsoft.com/en-us/cli/azure/functionapp>

3. <https://learn.microsoft.com/en-us/cli/azure/resource>
4. <https://cheatsheetseries.owasp.org/cheatsheets/HTTP-Headers-Cheat-Sheet.html>
5. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CORS>
6. <https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site-Request-Forgery-Prevention-Cheat-Sheet.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>16.1 Establish and Maintain a Secure Application Development Process</p> <p>Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v7	<p>18.1 Establish Secure Coding Practices</p> <p>Establish secure coding practices appropriate to the programming language and development environment being used.</p>			

2.5 Ensure Azure Key Vaults are Used to Store Secrets (Manual)

Profile Applicability:

- Level 2

Description:

Azure Key Vault will store multiple types of sensitive information such as encryption keys, certificate thumbprints, and Managed Identity Credentials. Access to these 'Secrets' can be controlled through granular permissions.

Rationale:

The credentials given to an application have permissions to create, delete, or modify data stored within the systems they access. If these credentials are stored within the application itself, anyone with access to the application or a copy of the code has access to them. Storing within Azure Key Vault as secrets increases security by controlling access. This also allows for updates of the credentials without redeploying the entire application.

Impact:

Integrating references to secrets within the key vault are required to be specifically integrated within the application code. This will require additional configuration to be made during the writing of an application, or refactoring of an already written one. There are also additional costs that are charged per 10000 requests to the Key Vault.

Audit:

Audit from Azure Portal

1. Login to Azure Portal.
2. In the expandable menu on the left go to **Key Vaults**.
3. View the Key Vaults listed.

Audit from Azure CLI

To list key vaults and/or HSMs within a subscription run the following command:

```
az keyvault list [--resource-type] --subscription  
<id_or_name_of_target_subscription>  
--resource-type could be either __vault__ or __hsm__ . When parameter is  
missing all types of vaults will be listed.
```

To list the **secrets** within a target key vaults run the following command:

```
az keyvault secret list [--vault-name / --id]
```

To list the certificates within a target key vault run the following command:

```
az keyvault certificate list [--vault-name / --id]
```

To list the keys within a target key vault run the following command:

```
az keyvault secret list [--vault-name / --id]
--id represents the full URI of the vault
--vault-name represents the name and must be present if --id is missing
```

Audit from PowerShell

To list key vaults within a subscription run the following command:

```
Get-AzKeyVault
```

To list all secrets in a key vault run the following command:

```
Get-AzKeyVaultSecret -VaultName '<vaultName>'
```

Remediation:

Remediation has 2 steps

1. Setup the Key Vault
2. Setup the App Service to use the Key Vault

Step 1: Set up the Key Vault

Remediate from Azure CLI

```
az keyvault create --name "<name>" --resource-group "<myResourceGroup>" --
location myLocation
```

Remediate from PowerShell

```
New-AzKeyvault -name <name> -ResourceGroupName <myResourceGroup> -Location
<myLocation>
```

Step 2: Set up the App Service to use the Key Vault

Sample JSON Template for App Service Configuration: [continues on next 3 pages]


```

{
  //...
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "name": "[variables('storageAccountName')]",
      //...
    },
    {
      "type": "Microsoft.Insights/components",
      "name": "[variables('appInsightsName')]",
      //...
    },
    {
      "type": "Microsoft.Web/sites",
      "name": "[variables('functionAppName')]",
      "identity": {
        "type": "SystemAssigned"
      },
      //...
      "resources": [
        {
          "type": "config",
          "name": "appsettings",
          //...
          "dependsOn": [
            "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]",
            "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
            "[resourceId('Microsoft.KeyVault/vaults/secrets',
variables('keyVaultName'), variables('storageConnectionStringName'))]",
            "[resourceId('Microsoft.KeyVault/vaults/secrets',
variables('keyVaultName'), variables('appInsightsKeyName'))]"
          ],
          "properties": {
            "AzureWebJobsStorage":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('storageConnectionStringResourceId')).secretUriWithVersio
n, '))]",
            "WEBSITE_CONTENTAZUREFILECONNECTIONSTRING":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('storageConnectionStringResourceId')).secretUriWithVersio
n, '))]",
            "APPINSIGHTS_INSTRUMENTATIONKEY":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('appInsightsKeyResourceId')).secretUriWithVersion,
''))]",
            "WEBSITE_ENABLE_SYNC_UPDATE_SITE": "true"
          //...
        }
      ],
    },
    {
      "type": "sourcecontrols",
      "name": "web",
      //...
      "dependsOn": [

```

```

        "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]",
        "[resourceId('Microsoft.Web/sites/config',
variables('functionAppName'), 'appsettings'))]"
    ],
    }
  ]
},
{
  "type": "Microsoft.KeyVault/vaults",
  "name": "[variables('keyVaultName')]",
  //...
  "dependsOn": [
    "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]"
  ],
  "properties": {
    //...
    "accessPolicies": [
      {
        "tenantId":
"[reference(concat('Microsoft.Web/sites/', variables('functionAppName'),
'/providers/Microsoft.ManagedIdentity/Identities/default'), '2015-08-31-
PREVIEW').tenantId]",
        "objectId":
"[reference(concat('Microsoft.Web/sites/', variables('functionAppName'),
'/providers/Microsoft.ManagedIdentity/Identities/default'), '2015-08-31-
PREVIEW').principalId]",
        "permissions": {
          "secrets": [ "get" ]
        }
      }
    ]
  },
  "resources": [
    {
      "type": "secrets",
      "name": "[variables('storageConnectionString')]",
      //...
      "dependsOn": [
        "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
        "[resourceId('Microsoft.Storage/storageAccounts',
variables('storageAccountName'))]"
      ],
      "properties": {
        "value":
"[concat('DefaultEndpointsProtocol=https;AccountName=',
variables('storageAccountName'), ';AccountKey=',
listKeys(variables('storageAccountResourceId'), '2015-05-01-preview').key1)]"
      }
    },
    {
      "type": "secrets",
      "name": "[variables('appInsightsKeyName')]",
      //...
      "dependsOn": [

```

```

        "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
        "[resourceId('Microsoft.Insights/components',
variables('appInsightsName'))]"
    ],
    "properties": {
        "value":
"[reference(resourceId('microsoft.insights/components/',
variables('appInsightsName')), '2015-05-01').InstrumentationKey]"
    }
}
]
}
]
}

```







Default Value:

By default, no Azure Key Vaults are created.

References:

1. <https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-3-manage-application-identities-securely-and-automatically>
3. <https://docs.microsoft.com/en-us/cli/azure/keyvault?view=azure-cli-latest>
4. <https://docs.microsoft.com/en-us/cli/azure/keyvault?view=azure-cli-latest>

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.			
v7	13.1 Maintain an Inventory Sensitive Information Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.			

2.6 Ensure App Service Environment is deployed with an internal load balancer (Automated)

Profile Applicability:

- Level 2

Description:

App Service Environment apps should not be reachable over public internet. To ensure apps deployed in an App Service Environment are not accessible over public internet, one should deploy App Service Environment with an IP address in virtual network. To set the IP address to a virtual network IP, the App Service Environment must be deployed with an internal load balancer.

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:

Audit from Azure Portal

1. Go to **App Service Environments**.
2. For each App Service Environment, ensure that **Virtual IP Type** is set to **Internal**.

Audit from Azure CLI

Run the following command to list App Service Environments:

```
az appservice ase list
```

For each App Service Environment, ensure that **internalLoadBalancingMode** is not set to **None**.

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:** [2d048aca-6479-4923-88f5-e2ac295d9af3](#) - **Name:** 'App Service Environment apps should not be reachable over public internet'

Remediation:

It is not possible to change the virtual IP configuration of a deployed App Service Environment.

When deploying an App Service Environment, next to **Virtual IP**, select **Internal: The endpoint is an internal load balancer (ILB ASE)**.







Default Value:

When deploying an App Service Environment, **Internal: The endpoint is an internal load balancer (ILB ASE)** is the default selected option for **Virtual IP**.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/environment/creation>

CIS Controls:

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

2.7 Ensure App Service Environment is provisioned with v3 or higher (Automated)

Profile Applicability:

- Level 1

Description:

Ensure App Service Environment is provisioned with v3 or higher to benefit from the latest enhancements.

Rationale:

Older versions of App Service Environment require manual management of Azure resources and have greater scaling limitations.

Impact:

Manual configuration may be required to complete the migration and to optimize your App Service plan SKU choice to meet your needs.

Audit:

Audit from Azure Portal

1. Go to **App Service Environments**.
2. Click the name of an App Service Environment.
3. Ensure that **Version** displays **App Service Environment v3** or higher.
4. Repeat steps 1-3 for each App Service Environment.

Audit from Azure CLI

Run the following command to list App Service Environments:

```
az appservice ase list
```

For each App Service Environment, ensure that **kind** is set to **ASEV3** or higher.

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:** [eb4d34ab-0929-491c-bbf3-61e13da19f9a](#) - **Name:** 'App Service Environment should be provisioned with latest versions'

Remediation:

Remediate from Azure Portal

When creating an App Service Environment from the portal, after clicking + **Add**, ensure that **Create App Service Environment v3** is displayed.

Default Value:

The default version is currently App Service Environment v3.







References:

1. <https://learn.microsoft.com/en-us/azure/app-service/environment/overview>
2. <https://azure.microsoft.com/en-gb/updates?id=App-Service-Environment-v1v2-Retirement-Update-1>
3. <https://learn.microsoft.com/en-us/azure/app-service/environment/auto-migration>
4. <https://learn.microsoft.com/en-us/cli/azure/appservice/ase>

Additional Information:

App Service Environment v1 and v2 were retired as of 31 August, 2024. As of September 1, 2024, Azure auto-migrated any remaining App Service Environment v1 and v2 on a best-effort basis.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	2.2 <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

2.8 Ensure App Service Environment has internal encryption enabled (Automated)

Profile Applicability:

- Level 2

Description:

The App Service Environment operates as a black box system where you cannot see the internal components or the communication within the system. To enable higher throughput, encryption is not enabled by default between internal components. The system is secure as the traffic is inaccessible to being monitored or accessed.

However, if you have a compliance requirement that requires complete encryption of the data path from end to end, you can enable encryption of the complete data path with a clusterSetting.

Rationale:

Setting InternalEncryption to true encrypts internal network traffic in your App Service Environment between the front ends and workers, encrypts the pagefile, and also encrypts the worker disks.

Impact:

At the point that this setting becomes desirable, an architectural review to evaluate a move to Azure Confidential Computing should be considered.

After the InternalEncryption clusterSetting is enabled, there can be an impact to your system performance and the additional resource demand will likely also increase the associated cost. When you make the change to enable InternalEncryption, your App Service Environment will be in an unstable state until the change is fully propagated. Complete propagation of the change can take a few hours to complete, depending on how many instances you have in your App Service Environment. Azure recommends that you do not enable InternalEncryption on an App Service Environment while it is in use. If you need to enable InternalEncryption on an actively used App Service Environment, Azure recommends that you divert traffic to a backup environment until the operation completes.

Audit:

Audit from Azure Portal

1. Go to **App Service Environments**.
2. Click the name of an App Service Environment.
3. Under **Settings**, click **Configuration**.
4. Ensure that **Internal encryption** is set to **On**.
5. Repeat steps 1-4 for each App Service Environment.

Audit from Azure CLI

Run the following command to list App Service Environments:

```
az appservice ase list
```

For each App Service Environment, ensure that **clusterSettings** includes:

```
{
  "name": "InternalEncryption",
  "value": "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:** [fb74e86f-d351-4b8d-b034-93da7391c01f](#) - **Name:** 'App Service Environment should have internal encryption enabled'

Remediation:

Remediate from Azure Portal

1. Go to **App Service Environments**.
2. Click the name of an App Service Environment.
3. Under **Settings**, click **Configuration**.
4. Next to **Internal encryption**, click the radio button next to **On**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each App Service Environment requiring remediation.





Default Value:

Internal encryption is disabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/environment/app-service-app-service-environment-custom-settings>
2. <https://learn.microsoft.com/en-us/cli/azure/appservice/ase>

CIS Controls:

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

2.9 Ensure App Service Environment has TLS 1.0 and 1.1 disabled (Automated)

Profile Applicability:

- Level 1

Description:

The TLS (Transport Layer Security) protocol secures the transmission of data over the internet using standard encryption technology. TLS versions 1.0 and 1.1 have been deprecated, and their use is generally discouraged. Disable all inbound TLS 1.0 and TLS 1.1 traffic for all the apps in an App Service Environment.

Rationale:

TLS 1.0 and 1.1 are outdated and vulnerable to security risks.

Impact:

Disallowing TLS 1.0 and 1.1 may affect compatibility with clients and backend services.

Audit:

Audit from Azure Portal

1. Go to **App Service Environments**.
2. Click the name of an App Service Environment.
3. Under **Settings**, click **Configuration**.
4. Ensure that **Allow TLS 1.0 and 1.1** is set to **Off**.
5. Repeat steps 1-4 for each App Service Environment.

Audit from Azure CLI

Run the following command to list App Service Environments:

```
az appservice ase list
```

For each App Service Environment, ensure that **clusterSettings** includes:

```
{
  "name": "DisableTls1.0",
  "value": "1"
}
```

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:** [d6545c6b-dd9d-4265-91e6-0b451e2f1c50](#) - **Name:** 'App Service Environment should have TLS 1.0 and 1.1 disabled'

Remediation:

Remediate from Azure Portal

1. Go to **App Service Environments**.
2. Click the name of an App Service Environment.
3. Under **Settings**, click **Configuration**.
4. Next to **Allow TLS 1.0 and 1.1**, click the radio button next to **Off**.
5. Click **Save**.
6. Click **Continue**.
7. Repeat steps 1-6 for each App Service Environment requiring remediation.





Default Value:

TLS 1.0 and 1.1 are allowed by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/environment/app-service-app-service-environment-custom-settings>
2. <https://learn.microsoft.com/en-us/cli/azure/appservice/ase>

CIS Controls:

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

2.10 Ensure App Service Environment has TLS cipher suite ordering configured (Automated)

Profile Applicability:

- Level 1

Description:

App Service Environment supports changing the cipher suite from the default. The default set of ciphers is the same set that is used in the multi-tenant App Service. Changing the cipher suite is only possible with App Service Environment, the single-tenant offering, not the multi-tenant offering, because changing it affects the entire App Service deployment.

There are two cipher suites that are required for an App Service Environment: `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` and `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`. Additionally, you should include the following cipher suites, which are required for TLS 1.3: `TLS_AES_256_GCM_SHA384` and `TLS_AES_128_GCM_SHA256`.

Rationale:

Configuring your App Service Environment to use only the ciphers it requires helps to keep the environment secure.

Impact:

If incorrect values are set for the cipher suite that SChannel cannot understand, all TLS communication to your server might stop functioning.

Audit:

Audit from Azure Portal

1. Go to **Resource Explorer**.
2. Locate an App Service Environment from the left pane.
3. Ensure the `clusterSettings` attribute includes:

```
{
  "name": "FrontEndSSLCipherSuiteOrder",
  "value":
  "TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_2
  56_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
}
```

4. Repeat steps 1-3 for each App Service Environment.

Audit from Azure CLI

Run the following command to list App Service Environments:

```
az appservice ase list
```

For each App Service Environment, ensure that **clusterSettings** includes:

```
{
  "name": "FrontEndSSLCipherSuiteOrder",
  "value":
  "TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
}
```

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:** [817dcf37-e83d-4999-a472-644eada2ea1e](#) - **Name:** 'App Service Environment should be configured with strongest TLS Cipher suites'

Remediation:

Remediate from Azure Portal

1. Go to **Resource Explorer**.
2. Locate an App Service Environment from the left pane.
3. In the right pane, click **Read/Write** to allow editing.
4. Click **Edit** to edit the resource.
5. Update the **clusterSettings** attribute to include:

```
{
  "name": "FrontEndSSLCipherSuiteOrder",
  "value":
  "TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
}
```

6. Click **PUT** to commit the change.
7. Repeat steps 1-7 for each App Service Environment requiring remediation.





Default Value:

TLS cipher suite ordering is not configured by default.

References:

1. <https://learn.microsoft.com/en-us/azure/app-service/environment/app-service-app-service-environment-custom-settings>
2. <https://learn.microsoft.com/en-us/cli/azure/appservice/ase>

CIS Controls:

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

3 Azure Container Instances

This section covers security best practice recommendations for Azure Container Instances.

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 Container Instances

Azure Product Page:

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

Azure Container Instances service overview:

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

Microsoft Cloud Security Baseline for Azure Container Instances:

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

3.1 Ensure Private Virtual Networks are used for Container Instances (Manual)

Profile Applicability:

- Level 1

Description:

Private Virtual Networks (vNets) ensure that services and hosts within the subscription environment are appropriately segmented in private subnets. Public IP addressing for container instances should be handled through a NAT gateway and/or Firewall. In addition to the use of a private vNet for container instances, ensure that a Network Security Group (NSG) is configured and applied to your container instance vNet. The NSG will need to be configured with inbound and outbound TCP/UDP traffic rules which reflect the needs of the services running in your container instance.

Rationale:

Network segmentation reduces threat surface and limits potential lateral movement in the case of breach. Container instances with Public IP addresses present significant threat surface and should be avoided.

Impact:

A well-architected Cloud network will require documentation and consideration for subnetting. The use of vNets and NSGs have a minimal impact on cost, but the use of Firewalls and public-facing gateways will increase that cost.

Audit:

Audit from Azure Portal

1. Go to **Container Instances**.
2. Select a named container instance.
3. Click on **Properties** under the Settings section.
4. Ensure the **IP address** property indicates **(Private)**.
5. Repeat these steps for each named container instance.

Audit from Azure CLI

Run the following command:

```
az container list
```

For each Container Instance, ensure **"type": "Private"** is indicated under the **"ipAddress"** section.

Remediation:

Container Instances which have been created with Public IP addresses will need to be re-created with private IP addresses. During the initial creation of a Container Instance, ensure that the Networking Type of "Private" is selected prior to creating the Container Instance.



Default Value:

By default, the "Public" Networking type is selected when creating a Container Instance from Azure Portal.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/container-instances-security-baseline?toc=%2Fazure%2Fcontainer-instances%2FTOC.json>
2. <https://learn.microsoft.com/en-us/azure/container-instances/container-instances-vnet>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			

3.2 Ensure a Managed Identity is used for interactions with other Azure services (Manual)

Profile Applicability:

- Level 1

Description:

For containers that require access to other resources, or other resources accessing a container, an identity/credential may be required. The Managed Identity prevents needing to store credentials in code within the Container Instance. There are two types of Managed Identities for Container Instances:

1. **System Assigned:** System Assigned Managed Identities provide an infrastructure integrated identity which is unique to the resource. It is assigned to the Container Instance and persists for the lifecycle of the resource. Permissions can be assigned, revoked, and tuned using Azure role-based access control.
2. **User Assigned:** User Assigned Managed Identities are not unique to the resource, and exist as independent Azure resources with their own lifecycle. If a Container Identity is decommissioned, the User Assigned Managed Identity will need to be decommissioned separately. User Assigned Managed Identities are not necessarily unique, and can be used across multiple resources.

Rationale:

Identities or credentials stored within a Container Instance or the code running on the Container Instance introduce a risk of compromise. If that identity or credential is stored in plain text, the risk is further amplified.

Impact:

To ensure that a Managed Identity is able to access a destination resource, the permissions and/or role assigned to that Managed Identity will need to be evaluated.

Audit:

Audit from Azure Portal

For each Container Instance that uses an identity or credential:

1. Open the **Container Instances** blade.
2. Select a named container instance.
3. Click on **Identity** under the Settings section.
4. Review the **System Assigned** and **User Assigned** tabs for assigned identities:
 - If using **System Assigned** identities, ensure status is set to **On**.
 - If using **User Assigned** identities, ensure only necessary user identities are assigned.

Audit from Azure CLI

Run the following command:

```
az container list
```

For each Container Instance that uses an identity or credential, ensure **"identity"**: is not **"null"**

Remediation:

Remediate from Azure Portal

For each Container Instance that requires an identity or credential:

1. Open the **Container Instances** blade.
2. Select a named container instance.
3. Click on **Identity** under the Settings section, then:
 - For a System Assigned identity, click the **System Assigned** tab then set status to **On**.
 - For User Assigned identities, click the **User Assigned** tab then click the **Add** button. Search for the required user managed identity, then click the **Add** button at the bottom of the window.

Remediate from Azure CLI

To assign Managed Identities to Container Instances by CLI, the Managed Identity will need to be specified at the time of creation. If a Container Instance requires a Managed Identity, but does not already have one, it will need to be re-created with the Managed Identity specified.

System Assigned Identity:

```
az container create -g <MyResourceGroup> --name <MyContainerInstanceName> --  
image <MyImage> --assign-identity [system]
```

User Assigned Identities:

```
az container create -g <MyResourceGroup> --name <MyContainerInstanceName> --  
image <MyImage> --assign-identity  
</subscriptions/MySubscriptionID/resourcegroups/MyResourceGroup/providers/Mic  
rosoft.ManagedIdentity/userAssignedIdentities/MyUserAssignedIdentity>
```

BOTH System and User Assigned Identities:

```
az container create -g <MyResourceGroup> --name <MyContainerInstanceName> --  
image <MyImage> --assign-identity [system]  
</subscriptions/MySubscriptionID/resourcegroups/MyResourceGroup/providers/Mic  
rosoft.ManagedIdentity/userAssignedIdentities/MyUserAssignedIdentity>
```




Default Value:

By default, Managed Identities are not configured on Container Instances.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/container-instances-security-baseline?toc=%2Fazure%2Fcontainer-instances%2FTOC.json#identity-management>
2. <https://learn.microsoft.com/en-us/azure/container-instances/using-azure-container-registry-mi>

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	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.			

3.3 Ensure the principle of least privilege is used when assigning roles to a Managed Identity (Manual)

Profile Applicability:

- Level 1

Description:

When using either a user-assigned or system-assigned managed identity, those identities may require a role or privilege assignment to perform a desired function. The roles or privileges assigned to that identity should be assigned with the principle of least privilege in mind - the identity is given the minimum levels of access or permissions needed to perform the job.

Rationale:

Threat actors may attempt to compromise service accounts as anomalous activity on these accounts can sometimes be more challenging to detect. Limiting the permissions or roles available to a managed identity or service account assists in mitigating the systemic exploitation that a service account can perform if compromised.

Impact:

All service accounts should be inventoried and reviewed from time to time for necessity and role or privilege assignment.

Audit:

Audit from Azure Portal

For each Container Instance that uses an identity or credential:

1. Open the **Container Instances** blade.
2. Select a named container instance.
3. Click on **Identity** under the Settings section.
4. Review the **System Assigned** and **User Assigned** tabs for assigned identities.

For a System Assigned identity, click on **Azure role assignments** and review the assigned roles for appropriate restriction.

For User assigned identities, click on the name of each User assigned managed identity, then click on **Azure role assignments** in the left panel to review assigned roles for appropriate restriction.

Remediation:

NOTE: Remediation will vary based on the needs of your environment. Before remediating, determine the scope and requirements of the Role Assignments necessary for your environment: <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

Remediate from Azure Portal

For each Container Instance that uses an identity or credential:

1. Open the **Container Instances** blade.
2. Select a named container instance.
3. Click on **Identity** under the Settings section.
4. Review the **System Assigned** and **User Assigned** tabs for assigned identities.



For a System Assigned identity, click on **Azure role assignments** and Add or Remove assigned roles for appropriate restriction.

For User assigned identities, click on the name of each User assigned managed identity, then click on **Azure role assignments** in the left panel to Add or Remove assigned roles for appropriate restriction.

References:

1. <https://learn.microsoft.com/en-us/azure/container-instances/container-instances-managed-identity>
2. <https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>
3. <https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal-managed-identity>
4. <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>6.8 <u>Define and Maintain Role-Based Access Control</u></p> <p>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.</p>			●

4 Azure CycleCloud

This section covers security best practice recommendations for Azure CycleCloud.

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 CycleCloud

Azure CycleCloud service overview:

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

4.1 Ensure SSL is configured for CycleCloud (Manual)

Profile Applicability:

- Level 1

Description:

The use of SSL ensures that data in transit to and from the Azure CycleCloud server is encrypted.

Rationale:

Encryption of data in transit provides integrity and confidentiality to that data. If unencrypted data is intercepted in transit it is highly vulnerable to exposure and exploitation.

Impact:

If using self-signed certificates, users accessing CycleCloud will receive a warning that the SSL certificate is untrusted; they will need to accept the certificate to access the web console. Depending on your environment and use of CycleCloud, you may wish to procure a signed and trusted certificate from a Certificate Authority.

Audit:

From SSH

1. Establish a secure shell session with the Azure CycleCloud server.
2. Navigate to the CycleCloud installation directory.
3. Use a text editor (e.g. Vim, Nano, Emacs) to open the `cycle_server.properties` file.
4. Review the file for the following properties:

```
webServerEnableHttps=true  
webServerRedirectHttp=true
```

Note that if these properties are defined in the file multiple times, only the **last** instance of that property definition will be in effect.

If either property is set to `false`, SSL is NOT configured for the CycleCloud server.

Remediation:

From SSH

1. Establish a secure shell session with the Azure CycleCloud server.
2. Navigate to the CycleCloud installation directory.
3. Use a text editor (e.g. Vim, Nano, Emacs) to open the `cycle_server.properties` file.
4. Edit the following properties to reflect `true`:

```
webServerEnableHttps=true  
webServerRedirectHttp=true
```

5. Save and exit from the text editor.
6. Restart the CycleCloud service to enable the new property definitions:

```
/opt/cycle_server/cycle_server restart
```





Default Value:

By default, CycleCloud is configured to use Java IO HTTPS with a Let's Encrypt SSL certificate, or self-signed certificate.

References:

1. <https://learn.microsoft.com/en-us/azure/cyclecloud/how-to/ssl-configuration?view=cyclecloud-8>
2. <https://learn.microsoft.com/en-us/azure/cyclecloud/concepts/security-best-practices?view=cyclecloud-8>

CIS Controls:

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

5 Azure Dedicated Host

No specific prescriptive guidance exists yet for Azure Dedicated Host.

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

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

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

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

Resources for Azure Dedicated Host

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/virtual-machines/dedicated-host/>

Azure Dedicated Host service overview:

- <https://learn.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts>

6 Azure Functions (Reference)

Coverage Location:

- Benchmark: "CIS Microsoft Azure **Compute Services** Benchmark" (this Benchmark)
- Section: **App Service**

Azure Functions, while considered a different product than App Service, relies on the same guidance provided by App Service.

Aside from the recommendations found in the section for App Service, no specific prescriptive guidance exists yet for Azure Functions.

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

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

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

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

Resources for Azure Functions

Azure Product Page:

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

Azure Functions service overview:

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

Microsoft Cloud Security Baseline for Azure Functions:

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

7 Azure Kubernetes Service (Reference)

Coverage Location:

- Benchmark: "[CIS Azure Kubernetes Service \(AKS\) Benchmark](https://www.cisecurity.org/benchmark/kubernetes)" - <https://www.cisecurity.org/benchmark/kubernetes>
- Community: [CIS Kubernetes Benchmarks](https://workbench.cisecurity.org/communities/43) - <https://workbench.cisecurity.org/communities/43>

This Microsoft Azure product—Azure Kubernetes Service (AKS)—is addressed in a separate, dedicated CIS Benchmark and Community.

Resources for Azure Kubernetes Service

Azure Product Page:

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

Azure Kubernetes Service service overview:

- <https://learn.microsoft.com/en-us/azure/aks/what-is-aks>

Microsoft Cloud Security Baseline for Azure Kubernetes Service:

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

8 Azure Quantum

No specific prescriptive guidance exists yet for Azure Quantum.

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

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

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

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

Resources for Azure Quantum

Azure Product Page:

- <https://azure.microsoft.com/en-us/solutions/quantum-computing/>

Azure Quantum service overview:

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

9 Azure Service Fabric

No specific prescriptive guidance exists yet for Azure Service Fabric.

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

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

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

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

Resources for Azure Service Fabric

Azure Product Page:

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

Azure Service Fabric service overview:

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

10 Azure Spot Virtual Machines (Reference)

Coverage Location:

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

Azure Spot Virtual Machines are a cost-advantaged implementation of Azure Virtual Machines and do not have specific security guidance. For secure configuration recommendations for Azure Spot Virtual Machines, please reference the "Virtual Machines" section of this benchmark.

Resources for Azure Spot Virtual Machines

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/virtual-machines/spot/>

Azure Spot Virtual Machines service overview:

- <https://learn.microsoft.com/en-us/azure/virtual-machines/spot-vms>

11 Azure Spring Apps (Retiring)

IMPORTANT NOTE: Azure Spring Apps plans are on a retirement path. Some plans have already been retired, and the remaining plans are in a three-year retirement period, to be retired on **March 31, 2028**. Microsoft is recommending the use of Azure Container Apps and Azure Kubernetes Service (AKS) instead. Please review Microsoft's announcement on this service retirement here: <https://learn.microsoft.com/en-us/azure/spring-apps/basic-standard/retirement-announcement>

No specific prescriptive guidance exists yet for Azure Spring Apps.

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

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

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

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

Resources for Azure Spring Apps

Azure Product Page:

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

Azure Spring Apps service overview:

- <https://learn.microsoft.com/en-us/azure/spring-apps/basic-standard/overview>

Microsoft Cloud Security Baseline for Azure Spring Apps:

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

12 Azure Virtual Desktop (Reference)

Coverage Location:

- Benchmark: ["CIS Microsoft Intune for Microsoft Windows Benchmarks" - https://www.cisecurity.org/benchmark/intune](https://www.cisecurity.org/benchmark/intune)
- Community: [CIS Microsoft Intune for Microsoft Windows - https://workbench.cisecurity.org/communities/116](https://workbench.cisecurity.org/communities/116)

This Microsoft Azure product—Azure Virtual Desktop—is addressed in a separate, dedicated CIS Benchmark and Community.

Resources for Azure Virtual Desktop

Azure Product Page:

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

Azure Virtual Desktop service overview:

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

Microsoft Cloud Security Baseline for Azure Virtual Desktop:

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

13 Azure VM Image Builder

No specific prescriptive guidance exists yet for Azure VM Image Builder.

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

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

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

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

Resources for Azure VM Image Builder

Azure Product Page:

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

Azure VM Image Builder service overview:

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

14 Azure VMware Solution

No specific prescriptive guidance exists yet for Azure VMware Solution.

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

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

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

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

Resources for Azure VMware Solution

Azure Product Page:

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

Azure VMware Solution service overview:

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

Microsoft Cloud Security Baseline for Azure VMware Solution:

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

15 Batch

This section covers security best practices recommendations for Azure Batch.

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 Batch

Azure Product Page:

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

Batch service overview:

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

Microsoft Cloud Security Baseline for Batch:

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

15.1 Ensure Batch account is set to use customer-managed keys to encrypt data (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:

Audit from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Navigate to **Batch accounts**

For each Batch account perform the following:

1. Under the **Settings** section, click on **Encryption**
2. Ensure that the **Customer-managed key** radio button is selected
3. Ensure that a key vault key is set and valid

If no key vault key is set, the configuration fails this audit procedure.

Audit from Azure CLI

The following command should return the Key URL and source Key Vault:

```
az batch account show --name <batch-account-name> --resource-group <resource-group-name> --query "keyVaultReference"
```

If the result is **null** or **Empty**, the configuration fails this audit procedure.

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:** [99e9ccd8-3db9-4592-b0d1-14b1715a4d8a](#) - **Name:** 'Azure Batch account should use customer-managed keys to encrypt data'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Navigate to **Batch accounts**

For each Batch account

1. Under the **Settings** section, click on **Encryption**
2. Select the **Customer-managed key** radio button
3. Use either **Enter key URI** or **Select from key vault** to select and set the encryption key.

Remediate from Azure CLI

```
# Link CMK to Batch account
az batch account set \
  --resource-group <resource_group_name> \
  --name <batch_account_name> \
  --encryption-key-identifier
https://<keyvault_name>.vault.azure.net/keys/<key_name>/<Version>
```

Remediate from PowerShell

```
Set-AzBatchAccount -ResourceGroupName <resource_group_name> -AccountName
<batch_account_name> `
  -KeyVaultReferenceId
"/subscriptions/<subscription_ID>/resourceGroups/<resource_group_name>/provid
ers/Microsoft.KeyVault/vaults/<keyvault_name>" `
  -KeyVaultReferenceUrl
"https://<keyvault_name>.vault.azure.net/keys/<key_name>"
```





Default Value:

Azure Batch accounts uses Microsoft-managed keys (service-managed encryption) for data at rest by default.

References:

1. <https://learn.microsoft.com/en-us/azure/batch/batch-customer-managed-key>

CIS Controls:

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

15.2 Ensure Batch pools disk encryption is set enabled (Automated)

Profile Applicability:

- Level 1

Description:

Azure Batch pools must have disk encryption enabled to protect data at rest on both OS and temporary disks, using Azure-managed encryption keys by default.

Rationale:

Enabling disk encryption meets compliance requirements, follows security best practices, and safeguards against unauthorized access to cached data and task outputs stored on VM disks.

Impact:

This ensures automatic encryption with minimal performance impact, though it requires pool recreation and is unsupported on Basic A-series VMs.

Audit:

Audit from Azure Portal

1. Login to Azure portal <https://portal.azure.com>
2. Navigate to **Batch Accounts**

For each Batch account perform the following:

1. Expand the **Features** section then click on **Pools**
2. For each Pool ID, click the name to open the pool
3. Under the **Configuration** section, check **Disk Encryption**

If the pool is encrypted, it should display "OS disk" and/or "Temporary disk" **encryption enabled**.

Audit from Azure CLI

Run the following commands:

```
# List all pools and their encryption status
az batch pool list \
  --account-name <batch-account-name> \
  --query "[].{id:id, encryption:deploymentConfiguration.virtualMachineConfiguration.diskEncryptionConfiguration}" \
  --output table
```

Expected Output: "OsDisk" and/or "TemporaryDisk" should be listed under **encryption.targets**.

Audit from PowerShell

Run the following command:

```
# Get Batch account context
$batchContext = Get-AzBatchAccount -AccountName "<batch-account-name>"

# List all pools and check encryption
Get-AzBatchPool -BatchContext $batchContext | ForEach-Object {
    $pool = $_
    $encryptionConfig =
$pool.DeploymentConfiguration.VirtualMachineConfiguration.DiskEncryptionConfi
guration
    [PSCustomObject]@{
        PoolId = $pool.Id
        OsDiskEncrypted = $encryptionConfig.Targets -contains "OsDisk"
        TempDiskEncrypted = $encryptionConfig.Targets -contains
"TemporaryDisk"
    }
}
```

Expected Output: OsDiskEncrypted and TempDiskEncrypted should be **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:** [1760f9d4-7206-436e-a28f-d9f3a5c8a227](#) - **Name:** 'Azure Batch pools should have disk encryption enabled'

Remediation:

NOTE: Encrypted pools must be created as replacements for unencrypted pools. Please ensure that necessary precautions are taken to backup and restore data from persistent disk pools.

Remediate from Azure Portal

1. Navigate to **Azure Batch accounts**
2. Select your Batch account
3. Click **Pools** in the **left menu**
4. For each unencrypted pool, click **Create new pool**
5. Under **Advanced settings**, enable **Disk encryption and select OS disk or All disks**
6. Configure all other settings to match your existing pool
7. Click **Create** to deploy the encrypted pool

8. Resize the old unencrypted pool to 0 nodes after verifying the new pool is operational

Repeat steps 4-8 for each unencrypted pool

Remediate from Azure CLI

1. Get pool configuration

```
config=$(az batch pool show --pool-id <pool-name> --query  
"{vmSize:vmSize,image:virtualMachineConfiguration.imageReference,nodeCount:targetDedicatedNodes}")
```

2. Create encrypted replacement

```
az batch pool create \  
  --id "<pool-name>-encrypted" \  
  --vm-size $(jq -r '.vmSize' <<< "$config") \  
  --image-reference "$(jq -r '.image.publisher + ":" + .image.offer + ":" +  
.image.sku + ":" + .image.version' <<< "$config")" \  
  --node-count $(jq -r '.nodeCount' <<< "$config") \  
  --disk-encryption-target OsDisk
```

3. Decommission old pool

```
az batch pool resize --pool-id <pool-name> --target-dedicated-nodes 0
```

Remediate from PowerShell

1. Get pool configuration

```
$pool = Get-AzBatchPool -Id "<pool-name>" -BatchContext $context
```

2. Create encrypted replacement

```
$newConfig = New-Object  
Microsoft.Azure.Commands.Batch.Models.PSPoolConfiguration  
$newConfig.VirtualMachineConfiguration =  
$pool.VirtualMachineConfiguration.Clone()  
$newConfig.VirtualMachineConfiguration.DiskEncryptionConfiguration = New-  
Object Microsoft.Azure.Commands.Batch.Models.PSDiskEncryptionConfiguration  
$newConfig.VirtualMachineConfiguration.DiskEncryptionConfiguration.Targets =  
"OsDisk"  
New-AzBatchPool -Id "<pool-name>-encrypted" -PoolConfiguration $newConfig -  
BatchContext $context
```

3. Decommission old pool

```
Set-AzBatchPool -Id "<pool-name>" -TargetDedicatedComputeNodes 0 -  
BatchContext $context
```

Expected Output: **Disk encryption Enabled**




Default Value:

Disk encryption is **disabled** by default for new Azure Batch pools.

References:

1. <https://docs.microsoft.com/en-us/azure/batch/disk-encryption>
2. <https://docs.microsoft.com/en-us/cli/azure/batch/pool#az-batch-pool-create>

CIS Controls:

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

15.3 Ensure local authentication methods for accounts are disabled (Automated)

Profile Applicability:

- Level 1

Description:

This recommendation disables local authentication and ensures that a centralized identity provider is used.

Rationale:

Identity and Authentication silos with stale or persistent keys and tokens can increase vulnerability and risk by preventing detection mechanisms from capturing anomalous activity and may not produce an auditable trail of evidence that can be used for pattern detection and forensic investigation. Centralized Identity providers such as Microsoft Entra ID are strongly preferred for all identity, authentication, authorization, and accountability (IAAA) systems and activities.

Audit:

Audit from Azure Portal

1. Login to Azure portal <https://portal.azure.com>
2. Navigate to **Batch Accounts**

For each Batch Account shown:

1. Click to open the Batch Account name
2. Under the Settings section, click on **Authentication modes**
3. In the main window, click the Authentication Mode drop-down list, and review which options are checked.

Expected Output: Only **Microsoft Entra ID** should be **checked**.

Audit from Azure CLI

Check Local Authentication Status for Batch Accounts

```
az batch account list \
--query "[].{name:name, resourceGroup:resourceGroup,
authModes:allowedAuthenticationModes}"
```

Expected Output:

- **SHOULD** contain "AAD" (Microsoft Entra ID)
- Should **NOT** contain "SharedKey" or other entries

Audit from PowerShell

List Authentication Methods for All Batch Accounts using script:

```
Get-AzBatchAccount | ForEach-Object
{
    $authModes = (Get-AzBatchAccount -Name $_.AccountName -ResourceGroupName
$_.ResourceGroupName).AllowedAuthenticationModes
    [PSCustomObject]@{
        AccountName = $_.AccountName
        ResourceGroup = $_.ResourceGroupName
        AuthenticationModes = $authModes -join ", "
    }
}
```

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:** [4dbc2f5c-51cf-4e38-9179-c7028eed2274](#) - **Name:** 'Configure Batch accounts to disable local authentication'
- **Policy ID:** [6f68b69f-05fe-49cd-b361-777ee9ca7e35](#) - **Name:** 'Batch accounts should have local authentication methods disabled'

Remediation:

Remediate from Azure Portal

1. Login to Azure portal <https://portal.azure.com>
2. Navigate to **Batch Accounts**

For each Batch Account shown:

1. Click to open the Batch Account name
2. Under the Settings section, click on **Authentication modes**
3. In the main window, click the Authentication Mode drop-down list
4. Check the box for **Microsoft Entra ID** (or other centralized IdP)
5. (If checked) Uncheck the box for **Shared Key**
6. (If checked) Uncheck the box for **Task Authentication Token**
7. Click **Save**





Default Value:

Local authentication methods are **enabled** by default.

References:

1. <https://learn.microsoft.com/en-us/azure/batch/security-best-practices#batch-account-authentication>

CIS Controls:

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

15.4 Ensure Private endpoints are considered for Batch accounts (Automated)

Profile Applicability:

- Level 2

Description:

Private endpoints for Azure Batch accounts ensure all network communication occurs over private networks rather than the public internet.

Rationale:

Configuring private endpoints for Azure Batch accounts ensures all network traffic remains within the Microsoft Azure backbone network, eliminating exposure to public internet threats. This meets zero-trust security principles by enforcing network-level isolation and reducing the attack surface. The configuration also enables precise network monitoring through Azure Network Watcher and NSG flow logs.

Impact:

Private endpoints come with an increased cost and complexity.

Audit:

Audit from Azure Portal

1. Login to Azure Portal <https://portal.azure.com/>
2. Navigate to **Batch Accounts**

For each Batch Account, perform the following:

1. Under Settings, click on **Networking**
2. Click the **Private access** tab
3. For each Private Endpoint listed, ensure that the connection state is **Approved**

Audit from Azure CLI

To list Private Endpoints from CLI:

```
az network private-endpoint list \
  --resource-group <RESOURCE_GROUP> \
  --query
"[?privateLinkServiceConnections[?contains(properties.privateLinkServiceId,
'Microsoft.Batch/batchAccounts/<BATCH_ACCOUNT_NAME>')] ] ]"
```

Expected: Should return at least one private endpoint configuration

Audit from PowerShell

To list Private Endpoints from PowerShell:

```
Get-AzPrivateEndpoint -ResourceGroupName <RESOURCE_GROUP> |  
    Where-Object { $_.PrivateLinkServiceConnections.PrivateLinkServiceId -  
match "Microsoft.Batch/batchAccounts/<BATCH_ACCOUNT_NAME>" }
```

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:** [0ef5aac7-c064-427a-b87b-d47b3ddcaf73](#) - **Name:** 'Configure Batch accounts with 'private endpoints''

Remediation:

Remediate from Azure Portal

1. Navigate to your Batch account
2. Under the Settings drop down, click **Networking**
3. Click the **Private access** tab
4. Click **+ Private endpoint**
5. Configure:
 - Virtual network and subnet
 - DNS integration (auto-approved recommended)
 - Target subresource: batchAccount

Remediate from Azure CLI

```
az network private-endpoint create \  
    --name batch-pe \  
    --resource-group <rg> \  
    --vnet-name <vnet> \  
    --subnet <subnet> \  
    --private-connection-resource-id /subscriptions/<sub-  
id>/resourceGroups/<rg>/providers/Microsoft.Batch/batchAccounts/<account> \  
    --group-id batchAccount \  
    --connection-name batch-connection
```





Default Value:

Private endpoints are not configured by default.

References:

1. <https://docs.microsoft.com/en-us/azure/batch/private-connectivity>

CIS Controls:

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

15.5 Ensure public network access is disabled for Batch accounts (Automated)

Profile Applicability:

- Level 1

Description:

Disabling public network access ensures all connectivity occurs through private endpoints or approved virtual networks.

Rationale:

Public network access exposes Batch accounts to internet threats like DDoS attacks and unauthorized access, violating Zero Trust principles and compliance requirements for secure data processing environments.

Impact:

A virtual network or private endpoint should be implemented for the Batch account prior to disabling public network access.

Audit:

Audit from Azure Portal

1. Login to <https://portal.azure.com>
2. For each Batch Account, click on the Batch account name
3. Navigate to the **Settings** drop-down, then click **Networking**.
4. Under the **Public access** tab, ensure that Public Network Access is set to **Disabled**.

Repeat for each Batch account in scope.

Audit from Azure CLI

```
az batch account show \
  --name <batch-account-name> \
  --resource-group <resource-group> \
  --query "publicNetworkAccess"
```

Audit from PowerShell

```
(Get-AzBatchAccount -Name "<batch-account-name>").PublicNetworkAccess
```

Expected Output: **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:** [c520cefc-285f-40f3-86e2-2efc38ef1f64](#) - **Name:** 'Configure Batch accounts to disable public network access'
- **Policy ID:** [74c5a0ae-5e48-4738-b093-65e23a060488](#) - **Name:** 'Public network access should be disabled for Batch accounts'

Remediation:

Remediation Procedure

1. Login to <https://portal.azure.com>
2. For each Batch Account, click on the Batch account name
3. Navigate to the **Settings** drop-down, then click **Networking**.
4. Under the **Public access** tab, ensure that Public Network Access is set to **Disabled**.
5. Click **Save**

Repeat for each Batch account in scope.

Remediate from Azure CLI

```
az batch account update \  
  --name <account-name> \  
  --resource-group <rg-name> \  
  --public-network-access Disabled
```

Remediate from PowerShell

```
Update-AzBatchAccount -Name <account-name> -ResourceGroupName <rg-name> -  
PublicNetworkAccess Disabled
```





Default Value:

Public network access is **enabled** by default for new Batch accounts.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/batch-security-baseline#ns-4>
2. <https://learn.microsoft.com/en-us/azure/batch/private-connectivity>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 <u>Perform Traffic Filtering Between Network Segments</u> Perform traffic filtering between network segments, where appropriate.			
v7	14.2 <u>Enable Firewall Filtering Between VLANs</u> Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.			

15.6 Ensure private DNS zones for private endpoints that connect to Batch accounts are configured. (Manual)

Profile Applicability:

- Level 2

Description:

Private DNS zones for Azure Batch private endpoints provide secure internal name resolution, preventing public internet exposure. When a private endpoint is created for a Batch account, Azure requires a private DNS zone (privatelink..batch.azure.com) to map the Batch service's domain name to a private IP address within your virtual network (VNet).

Rationale:

To enable secure and private access to Azure Batch accounts, private DNS zones must be properly configured for private endpoints so as not to expose them publicly and allow for internal name resolution. Proper configuration of DNS provides assurance that DNS resolves to private IPs, reducing data exposure risk and support for security policy adherence. In the absence of proper DNS configuration, Batch services are open to connectivity failure, job interruption, or misconfigured public internet routing. Well-meshed private DNS zones hold traffic within the virtual network as intended, as a Zero Trust architecture and regulatory standard would dictate. Organizations need to audit and automate the configurations for secure and stable Batch processing.

Impact:

NOTE: This recommendation assumes that a Private DNS Zone already exists. If one has not yet been created for Batch accounts [e.g. privatelink.batch.azure.com], that must be completed before it can be assigned to a Batch account's Private Endpoint.

Network architecture must be carefully considered when deploying Private DNS Zones. DNS Zones should be used to associate like services. Private DNS zones should not be used to resolve public endpoints.

Audit:

Audit from Azure Portal

1. Login to Azure portal <https://portal.azure.com>
2. Navigate to **Batch accounts** in the Azure portal

For each batch account perform the following:

1. Expand **Settings** then click on **Networking**
2. Click the **Private access** tab,

If no Private endpoints exist, the configuration fails this audit procedure.
For each Private endpoint perform the following:

1. Click the name of the Private Endpoint
2. Expand **Settings** then click on **DNS Configuration**
3. Scroll to the bottom where a table of **Configuration entries** is found

Ensure that there is an entry populated in the **Private DNS Zone** column (e.g. **privatelink.batch.azure.com**)

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://learn.microsoft.com/en-us/azure/batch/private-connectivity#azure-policy>

- **Policy ID:** [4ec38ebc-381f-45ee-81a4-acbc4be878f8](#) - **Name:** 'Azure Batch accounts should use private DNS zones for 'private endpoints''

Remediation:

NOTE: This instruction assumes a Private Endpoint already exists for the Batch Account, and that a Private DNS Zone has already been created.

Remediate from Azure Portal

1. Login to Azure portal <https://portal.azure.com>
2. Navigate to **Batch accounts** in the Azure portal

For each batch account perform the following:

1. Expand **Settings** then click on **Networking**
2. Click the **Private access** tab,

*[If no Private Endpoints exist, one must be created before proceeding. Instruction for configuring Private Endpoints on Batch Accounts can be found in the recommendation titled "**Ensure to Configure Batch accounts with private endpoints**"]*

For each Private endpoint perform the following:

1. Click the name of the Private Endpoint
2. Expand **Settings** then click on **DNS Configuration**
3. Click the **+ Add Configuration** button
4. Select each field appropriately (e.g. Private DNS zone "privatelink.batch.azure.com" - other zone names in additional information below) and enter a custom Configuration Name if desired

5. Click the **Add** button then allow a moment for deployment

Refresh the DNS Configuration page, then scroll down and ensure an entry exists (e.g. "privatelink.batch.azure.com") under the **Private DNS zone** column in the Configuration entry table.

Default Value:

Azure DNS zones are not configured by default.

References:

1. <https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns>
2. <https://learn.microsoft.com/en-us/azure/batch/private-connectivity>
3. Commercial Zone Names: <https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#compute>
4. Government Zone Names: <https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#compute-1>
5. China Zone Names: <https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns#compute-2>

Additional Information:

Zone Names for resource type: Azure Batch (Microsoft.Batch/batchAccounts)

Azure Commercial Cloud:

1. Subresource: batchAccount
 - Private DNS Zone name: **privatelink.batch.azure.com**
 - Public DNS zone forwarders: **<regionName>.batch.azure.com**
2. Subresource: nodeManagement
 - Private DNS Zone name: **privatelink.batch.azure.com**
 - Public DNS zone forwarders: **<regionName>.service.batch.azure.com**





Azure Government Cloud:

1. Subresource: batchAccount
 - Private DNS Zone name: **privatelink.batch.usgovcloudapi.net**
 - Public DNS zone forwarders: **<regionName>.batch.usgovcloudapi.net**
2. Subresource: nodeManagement
 - Private DNS Zone name: **privatelink.batch.usgovcloudapi.net**
 - Public DNS zone forwarders: **<regionName>.service.batch.usgovcloudapi.net**

Azure China Cloud:

1. Subresource: batchAccount
 - Private DNS Zone name: `privatelink.batch.chinacloudapi.cn`
 - Public DNS zone forwarders: `<regionName>.batch.chinacloudapi.cn`
2. Subresource: nodeManagement
 - Private DNS Zone name: `privatelink.batch.chinacloudapi.cn`
 - Public DNS zone forwarders:
`<regionName>.service.batch.chinacloudapi.cn`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>12.2 Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	<u>11.1 Maintain Standard Security Configurations for Network Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.			

15.7 Ensure Diagnostics settings logs for Batch accounts are enabled (Automated)

Profile Applicability:

- Level 1

Description:

Azure Batch resource logs give important operational data such as job scheduling, pool management, and node communication. Having these logs enabled is necessary for monitoring, troubleshooting, and compliance auditing.

Rationale:

Enable resource logging for:

- Operational Visibility — Keep track of any job failures, node allocation issues, or API activities.
- Security Compliance — Needed for audits (ISO 27001, SOC 2, GDPR).
- Forensic Investigations — Acts as evidence in case of security incidents or performance bottlenecks.

Impact:

Costs for monitoring varies with Log Volume and storage destination. 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.

Retention is not addressed in this recommendation and should be considered depending on the needs of your organization. A 30-day minimum is recommended and longer may be required depending on the security or compliance framework your organization is following.

Audit:

Audit from Azure Portal

1. Login to Azure portal <https://portal.azure.com>
2. Go to **Batch Accounts**

For each Batch account perform the following:

1. Expand the **Monitoring** section and click on **Diagnostic settings**

If no named **Diagnostic setting** exists in the table, the configuration fails this audit procedure.

Review the named **Diagnostics settings** in the table to ensure that the following categories are enabled:

- ServiceLog (Tracks Batch service operations)
- AuditLog (Records management-plane activities)

Ensure that each is configured to send to a valid destination:

- Log Analytics workspace (Recommended for querying)
- Storage account (For long-term retention)
- Event Hub (For real-time streaming)

Audit from Azure CLI

```
az batch account list --query "[].id" | xargs -I {} az monitor diagnostic-  
settings list --resource {} --query "value[].{account:{split('/')[8]},  
name:name, enabled:logs[?enabled]}" -o tsv
```

Audit from PowerShell

```
Get-AzBatchAccount | ForEach-Object {  
    $settings = Get-AzDiagnosticSetting -ResourceId $_.Id  
    [PSCustomObject]@{  
        AccountName = $_.AccountName  
        HasDiagnostics = ($settings -ne $null)  
        LogsEnabled = ($settings.Logs | Where-Object Enabled).Count -gt 0  
    }  
}
```

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:** [428256e6-1fac-4f48-a757-df34c2b3336d](#) - **Name:** 'Resource logs in Batch accounts should be enabled'

Remediation:

Remediate from Azure Portal

1. Login to Azure portal <https://portal.azure.com>
2. Go to **Batch Accounts**

For each Batch account perform the following:

1. Expand the **Monitoring** section and click on **Diagnostic settings**
2. Click **+Add diagnostic setting**
3. Enter an appropriate name, then ensure that the following categories are checked:
 - ServiceLog (Tracks Batch service operations)
 - AuditLog (Records management-plane activities)
4. Configure to send to a valid destination based on what is used within your tenant:
 - Log Analytics workspace (Recommended for querying)
 - Storage account (For long-term retention)
 - Event Hub (For real-time streaming)
5. Click **Save**

Remediate from Azure CLI

```
az monitor diagnostic-settings create \  
  --name "<batch_logs_name>" \  
  --resource $(az batch account show --name <batch_account_name> --resource-  
group <resource_group_name> --query id -o tsv) \  
  --logs '[{"category": "AuditLog", "enabled": true}, {"category":  
"ServiceLog", "enabled": true}]' \  
  --workspace $(az monitor log-analytics workspace show --resource-group  
<resource_group_name> --name <workspace_name> --query id -o tsv) \  

```

Remediate from PowerShell

```
$batchAccountId = (Get-AzBatchAccount -AccountName "<batch_account_name>" -  
ResourceGroupName "<resource_group_name>").Id  
New-AzDiagnosticSetting -Name "BatchLogs" -ResourceId $batchAccountId -Log  
@(@{Category="AuditLog";Enabled=$true},  
@{Category="ServiceLog";Enabled=$true}) -WorkspaceId (Get-  
AzOperationalInsightsWorkspace -Name "<workspace_name>").ResourceId  

```

Default Value:

Resource logs are not configured by default.

References:

1. <https://learn.microsoft.com/en-us/azure/batch/monitoring-overview#diagnostic-logs>
2. <https://learn.microsoft.com/en-us/azure/batch/batch-diagnostics#service-logs>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	8.9 <u>Centralize Audit Logs</u> Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.5 <u>Central Log Management</u> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

16 Linux Virtual Machines (Reference)

Coverage Location:

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

Linux Virtual Machines in Azure are deployed through the Virtual Machines service. Recommendations for the Virtual Machines service can be found in the "Virtual Machines" section of this Benchmark. Please note that for the purposes of this benchmark, recommendations are written from the perspective of securing the underlying Azure infrastructure, not the operating system running on the infrastructure.

For guidance and security best practice recommendations for the Linux operating system, please refer to the following resources:

- CIS Benchmarks Website (Linux can be found under "Operating Systems"):
<https://www.cisecurity.org/cis-benchmarks>
- CIS Workbench Communities* for Linux:
<https://workbench.cisecurity.org/communities/public?q=linux>

*Please note that there are over 20 Linux Communities which are based on commonly used distributions, and there is a CIS Distribution Independent Linux Benchmark which provides distribution independent recommendations.

Resources for Linux Virtual Machines

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/virtual-machines/linux/>

Virtual Machines service overview:

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

17 SQL Server on Azure Virtual Machines (Reference)

Coverage Location:

- Benchmark: "CIS Microsoft Azure **Database Services** Benchmark"
- Section: **SQL Server on Azure Virtual Machines**

Recommendations for the SQL Server on Azure Virtual Machines service can be found in the "SQL Server on Azure Virtual Machines" section of the CIS Microsoft Azure Database Services Benchmark.

Resources for SQL Server on Azure Virtual Machines

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/virtual-machines/sql-server/>

SQL Server on Azure Virtual Machines service overview:

- <https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-on-azure-vm-iaas-what-is-overview>
- <https://learn.microsoft.com/en-us/azure/azure-sql/virtual-machines/linux/sql-server-on-linux-vm-what-is-iaas-overview>

18 Static Web Apps (Reference)

Coverage Location:

- Benchmark: "CIS Microsoft Azure **Compute Services** Benchmark" (this Benchmark)
- Section: **App Service**

Static Web Apps, while considered a different product than App Service, relies on the same guidance provided by App Service.

Aside from the recommendations found in the section for App Service, no specific prescriptive guidance exists yet for Static Web Apps.

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

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

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

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

Resources for Static Web Apps

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/app-service/static/>

Static Web Apps service overview:

- <https://learn.microsoft.com/en-us/azure/static-web-apps/overview>

19 Virtual Machine Scale Sets

No specific prescriptive guidance exists yet for Virtual Machine Scale Sets.

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

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

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

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

Resources for Virtual Machine Scale Sets

Azure Product Page:

- <https://azure.microsoft.com/en-us/products/virtual-machine-scale-sets/>

Virtual Machine Scale Sets service overview:

- <https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview>

Microsoft Cloud Security Baseline for Virtual Machine Scale Sets:

- <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/virtual-machine-scale-sets-security-baseline>

20 Virtual Machines

This section covers security best practice recommendations for Virtual Machines.

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 Virtual Machines

Azure Product Page:

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

Virtual Machines service overview:

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

Microsoft Cloud Security Baseline for Linux Virtual Machines:

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

Microsoft Cloud Security Baseline for Windows Virtual Machines:

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

20.1 Ensure Virtual Machines are utilizing Managed Disks (Automated)

Profile Applicability:

- Level 1

Description:

Migrate blob-based VHDs to Managed Disks on Virtual Machines to exploit the default features of this configuration. The features include:

1. Default Disk Encryption
2. Resilience, as Microsoft will managed the disk storage and move around if underlying hardware goes faulty
3. Reduction of costs over storage accounts

Rationale:

Managed disks are by default encrypted on the underlying hardware, so no additional encryption is required for basic protection. It is available if additional encryption is required. Managed disks are by design more resilient that storage accounts.

For ARM-deployed Virtual Machines, Azure Adviser will at some point recommend moving VHDs to managed disks both from a security and cost management perspective.

Impact:

There are additional costs for managed disks based off of disk space allocated. When converting to managed disks, VMs will be powered off and back on.

Audit:

Audit from Azure Portal

1. Using the search feature, go to **Virtual Machines**
2. Click the **Manage view** dropdown, then select **Edit columns**
3. Add **Uses managed disks** to the selected columns
4. Select **Save**
5. Ensure all virtual machines listed are using managed disks

Audit from PowerShell

```
Get-AzVM | ForEach-Object {"Name: " + $_.Name; "ManagedDisk Id: " +  
$_.StorageProfile.OsDisk.ManagedDisk.Id; ""}
```

Example output:

```
Name: vm1
ManagedDisk Id: /disk1/id

Name: vm2
ManagedDisk Id: /disk2/id
```

If the 'ManagedDisk Id' field is empty the os disk for that vm is not managed.

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:** [06a78e20-9358-41c9-923c-fb736d382a4d](#) - **Name:** 'Audit VMs that do not use managed disks'

Remediation:

Remediate from Azure Portal

1. Using the search feature, go to **Virtual Machines**
2. Select the virtual machine you would like to convert
3. Select **Disks** in the menu for the VM
4. At the top select **Migrate to managed disks**
5. You may follow the prompts to convert the disk and finish by selecting **Migrate** to start the process

NOTE VMs will be stopped and restarted after migration is complete.

Remediate from PowerShell

```
Stop-AzVM -ResourceGroupName $rgName -Name $vmName -Force
ConvertTo-AzVMManagedDisk -ResourceGroupName $rgName -VMName $vmName
Start-AzVM -ResourceGroupName $rgName -Name $vmName
```




Default Value:

Managed disks or are an option upon the creation of VMs.

References:

1. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/convert-unmanaged-to-managed-disks>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default>
3. <https://docs.microsoft.com/en-us/azure/virtual-machines/fq-for-disks>
4. <https://azure.microsoft.com/en-us/pricing/details/managed-disks/>

CIS Controls:

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

20.2 Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that OS disks (boot volumes) and data disks (non-boot volumes) are encrypted with CMK (Customer Managed Keys). Customer Managed keys can be either ADE or Server Side Encryption (SSE).

Rationale:

Encrypting the IaaS VM's OS disk (boot volume) and Data disks (non-boot volume) ensures that the entire content is fully unrecoverable without a key, thus protecting the volume from unwanted reads. PMK (Platform Managed Keys) are enabled by default in Azure-managed disks and allow encryption at rest. CMK is recommended because it gives the customer the option to control which specific keys are used for the encryption and decryption of the disk. The customer can then change keys and increase security by disabling them instead of relying on the PMK key that remains unchanging. There is also the option to increase security further by using automatically rotating keys so that access to disk is ensured to be limited. Organizations should evaluate what their security requirements are, however, for the data stored on the disk. For high-risk data using CMK is a must, as it provides extra steps of security. If the data is low risk, PMK is enabled by default and provides sufficient data security.

Impact:

Using CMK/BYOK will entail additional management of keys.

NOTE: You must have your key vault set up to utilize this.

Audit:

Audit from Azure Portal

1. Go to **Virtual machines**.
2. For each virtual machine, go to **Settings**.
3. Click on **Disks**.
4. Ensure that the **OS disk** and **Data disks** have encryption set to CMK.

Audit from PowerShell

```
$ResourceGroupName="yourResourceGroupName"
$DiskName="yourDiskName"

$disk=Get-AzDisk -ResourceGroupName $ResourceGroupName -DiskName $DiskName
$disk.Encryption.Type
```

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:** [ca88aad6-6e2b-416c-9de2-5a0f01d1693f](#) - **Name:** 'Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost'
- **Policy ID:** [3dc5edcd-002d-444c-b216-e123bbfa37c0](#) - **Name:** 'Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost'

Remediation:

Remediate from Azure Portal

Note: Disks must be detached from VMs to have encryption changed.

1. Go to **Virtual machines**
2. For each virtual machine, go to **Settings**
3. Click on **Disks**
4. Click the ellipsis (...), then click **Detach** to detach the disk from the VM
5. Now search for **Disks** and locate the unattached disk
6. Click the disk then select **Encryption**
7. Change your encryption type, then select your encryption set
8. Click **Save**
9. Go back to the VM and re-attach the disk

Remediate from PowerShell

```
$KVRGName = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MySecureVM';
$KeyVaultName = 'MySecureVault';
$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName
$KVRGName;
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
$KeyVaultResourceId = $KeyVault.ResourceId;

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName
-DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $KeyVaultResourceId;
```

NOTE:

During encryption it is likely that a reboot will be required. It may take up to 15 minutes to complete the process.

For Linux machines you may need to set the **-skipVmBackup** parameter.




Default Value:

By default, Azure disks are encrypted using SSE with PMK.

References:

1. <https://docs.microsoft.com/azure/security/fundamentals/azure-disk-encryption-vmss-vmss>
2. <https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json>
3. <https://docs.microsoft.com/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-resthttps://docs.microsoft.com/azure/virtual-machines/windows/disk-encryption-portal-quickstart>
4. <https://docs.microsoft.com/en-us/rest/api/compute/disks/delete>
5. <https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings>
6. <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>
7. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell>
8. <https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption>

CIS Controls:

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

20.3 Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that unattached disks in a subscription are encrypted with a Customer Managed Key (CMK).

Rationale:

Managed disks are encrypted by default with Platform-managed keys. Using Customer-managed keys may provide an additional level of security or meet an organization's regulatory requirements. Encrypting managed disks ensures that its entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads. Even if the disk is not attached to any of the VMs, there is always a risk where a compromised user account with administrative access to VM service can mount/attach these data disks, which may lead to sensitive information disclosure and tampering.

Impact:

NOTE: You must have your key vault set up to utilize this. Encryption is available only on Standard tier VMs. This might cost you more.

Utilizing and maintaining Customer-managed keys will require additional work to create, protect, and rotate keys.

Audit:

Audit from Azure Portal

1. Go to **Disks**
2. Click on **Add Filter**
3. In the **filter** field select **Disk state**
4. In the **Value** field select **Unattached**
5. Click **Apply**
6. for each disk listed ensure that **Encryption type** in the **encryption** blade is 'Encryption at-rest with a customer-managed key'

Audit from Azure CLI

Ensure command below does not return any output.

```
az disk list --query '[? diskstate == `Unattached`].{encryptionSettings: encryptionSettings, name: name}' -o json
```

Sample Output:

```
[
  {
    "encryptionSettings": null,
    "name": "<Disk1>"
  },
  {
    "encryptionSettings": null,
    "name": "<Disk2>"
  }
]
```

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:** [ca91455f-eace-4f96-be59-e6e2c35b4816](#) - **Name:** 'Managed disks should be double encrypted with both platform-managed and customer-managed keys'

Remediation:

If data stored in the disk is no longer useful, refer to Azure documentation to delete unattached data disks at:

```
-https://docs.microsoft.com/en-us/rest/api/compute/disks/delete
-https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-delete
```

If data stored in the disk is important, to encrypt the disk refer to azure documentation at:

```
-https://docs.microsoft.com/en-us/azure/virtual-machines/disks-enable-customer-managed-keys-portal
-https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings
```

Default Value:




By default, managed disks are encrypted with a Platform-managed key.

References:

1. <https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vmss-vmss>
2. <https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json>
3. <https://docs.microsoft.com/en-us/rest/api/compute/disks/delete>
4. <https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-delete>

5. <https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings>
6. <https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-update>
7. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>

CIS Controls:

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

20.4 Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Automated)

Profile Applicability:

- Level 1

Description:

Virtual Machine Disks and snapshots can be configured to allow access from different network resources.

Rationale:

The setting 'Enable public access from all networks' is, in many cases, an overly permissive setting on Virtual Machine Disks that presents atypical attack, data infiltration, and data exfiltration vectors. If a disk to network connection is required, the preferred setting is to 'Disable public access and enable private access.'

Impact:

The setting 'Disable public access and enable private access' will require configuring a private link (URL in references below).

The setting 'Disable public and private access' is most secure and preferred where disk network access is not needed.

Audit:

Audit from Azure Portal

Part A. Select the Virtual Machine to Evaluate

1. Using the search bar, search for and open the **Virtual Machines** service.
2. Click on the name of the Virtual Machine to be audited.

Part B. Evaluate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the **Settings** menu item and click **Disks**.
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the **Settings** menu item, and click **Networking**.

Ensure that Network access is **NOT** set to **Enable public access from all networks**.

Repeat Part B for each Disk attached to a VM.

Repeat Parts A and B to evaluate all Disks in all VMs.

Audit from PowerShell

For each managed disk, run the following PowerShell command:

```
Get-AzDisk -ResourceGroupName '<resource group name>' -DiskName '<disk name>'
```

Ensure the **PublicNetworkAccess** setting is **Disabled** and the **NetworkAccessPolicy** is set to **AllowPrivate** or **DenyAll**.

Audit from Azure CLI

For each managed disk, run the following command:

```
az disk show --disk-name '<disk name>' --resource-group '<resource group name>'
```

Ensure the **publicNetworkAccess** setting is set to **Disabled** and the **networkAccessPolicy** setting is set to **AllowPrivate** or **DenyAll**.

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:** [8405fdab-1faf-48aa-b702-999c9c172094](#) - **Name:** 'Managed disks should disable public network access'

Remediation:

Remediate from Azure Portal

Part A. Select the Virtual Machine to Remediate

1. Using the search bar, search for and open the **Virtual Machines** service.
2. Click on the name of the Virtual Machine to be remediated.

Part B. Remediate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the **Settings** menu item and click **Disks**.
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the **Settings** menu item, and click **Networking**.

Under Network access, select the radio button for either:

- Disable public access and enable private access
- Disable public and private access

Repeat Part B for each Disk attached to a VM.
Repeat Parts A and B to remediate all Disks in all VMs.

Remediate from PowerShell

To disable **PublicNetworkAccess** and to set a **DenyAll** setting for the disk's **NetworkAccessPolicy** for each managed disk, run the following command:

```
$disk = Get-AzDisk -ResourceGroupName '<resource group name>' -DiskName '<disk name>'
$disk.NetworkAccessPolicy = 'DenyAll'
$disk.PublicNetworkAccess = 'Disabled'
Update-AzDisk -ResourceGroup '<resource group name>' -DiskName $disk.Name -Disk $disk
```

To disable **PublicNetworkAccess** and to set an **AllowPrivate** setting for the disk's **NetworkAccessPolicy** for each managed disk, run the following command:

```
$disk = Get-AzDisk -ResourceGroupName '<resource group name>' -DiskName '<disk name>'
$disk.NetworkAccessPolicy = 'AllowPrivate'
$disk.PublicNetworkAccess = 'Disabled'
$disk.DiskAccessId = '/subscriptions/<subscription ID>/resourceGroups/<resource group name>/providers/Microsoft.Compute/diskAccesses/<private disk access name>'
Update-AzDisk -ResourceGroup '<resource group name>' -DiskName $disk.Name -Disk $disk
```

Remediate from Azure CLI

To configure a disk to allow private access only, run the following command making sure you have the **Disk Access ID** from a private disk access end point.

```
az disk update --name <managed disk name> --resource-group <resource group name> --network-access-policy AllowPrivate --disk-access <disk access ID>
```

To completely disable public and private access for a disk, run the following command (still in preview) for each disk:

```
az disk update --name <managed disk name> --resource-group <resource group name> --public-network-access Disabled --network-access-policy DenyAll
```

Default Value:







By default, Disk Network access is set to **Enable public access from all networks**.

References:

1. <https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-private-links-for-import-export-portal>
2. <https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disks-export-import-private-links-cli>

3. <https://learn.microsoft.com/en-us/azure/virtual-machines/disks-restrict-import-export-overview>

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.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

20.5 Ensure that 'Enable Data Access Authentication Mode' is 'Checked' (Automated)

Profile Applicability:

- Level 1

Description:

Data Access Authentication Mode provides a method of uploading or exporting Virtual Machine Disks.

Rationale:

Enabling **data access authentication mode** adds a layer of protection using an Entra ID role to further restrict users from creating and using Secure Access Signature (SAS) tokens for exporting a detached managed disk or virtual machine state. Users will need the **Data operator for managed disk** role within Entra ID in order to download a VHD or VM Guest state using a secure URL.

Impact:

To apply this setting, the virtual machine to which the disk or disks are attached will need to be powered down and have its disk detached. Users without the **Data operator for managed disk** role within Entra ID will not be able to export VHD or VM guest state using the secure download URL.

The following restrictions apply and must be considered when determining if this recommendation is appropriate for your environment:

- VHDs can't be uploaded to empty snapshots.
- Azure Backup doesn't currently support disks secured with Microsoft Entra ID.
- Azure Site Recovery doesn't currently support disks secured with Microsoft Entra ID.

Audit:

Audit from Azure Portal

Part A. Select the Virtual Machine to Evaluate

1. Using the search bar, search for and open the **Virtual Machines** service.
2. Click on the name of the Virtual Machine to be audited.

Part B. Evaluate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the **Settings** menu item and click **Disks**.
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the **Settings** menu item, and click **Disk Export**.

Ensure that **Enable Data Access Authentication Mode** is checked.

Repeat Part B for each Disk attached to a VM.

Repeat Parts A and B to evaluate all Disks in all VMs.

Audit from PowerShell

Run the following command for each disk:

```
Get-AzDisk -ResourceGroupName <resource_group_name> -DiskName <disk_name>
```

Ensure the **DataAccessAuthMode** setting displays **AzureActiveDirectory** next to it.

Audit from Azure CLI

Run the following command for each disk:

```
az disk show --disk-name <disk_name> --resource-group <resource_group_name>
```

Ensure the **dataAccessAuthMode** setting is set to **AzureActiveDirectory**

Remediation:

Remediate from Azure Portal

Part A. Select the Virtual Machine to Remediate

1. Using the search bar, search for and open the **Virtual Machines** service.
2. Click on the name of the Virtual Machine to be remediated.

Part B. Remediate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the **Settings** menu item and click **Disks**.
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the **Settings** menu item, and click **Disk Export**.

check the checkbox next to **Enable Data Access Authentication Mode**.

Repeat Part B for each Disk attached to a VM.

Repeat Parts A and B to remediate all Disks in all VMs.

Remediate from PowerShell

Ensure that each disk is detached from its associated **Virtual Machine** before proceeding. Once detached, run the following for each disk:

```
$disk = Get-AzDisk -ResourceGroupName <resource_group_name> -DiskName <disk_name>
$disk.DataAccessAuthMode = 'AzureActiveDirectory'
Update-AzDisk -ResourceGroup <resource_group_name> -DiskName $disk.Name -Disk $disk
```

Remediate from Azure CLI

Ensure that each disk is detached from its associated **Virtual Machine** before proceeding. Once detached, run the following for each disk:

```
az disk update --name <disk_name> --resource-group <resource_group_name> --data-access-auth-mode AzureActiveDirectory
```







Default Value:

By default, Data Access Authentication Mode is **Disabled**.

References:

1. <https://learn.microsoft.com/en-us/azure/virtual-machines/linux/download-vhd?tabs=azure-portal#secure-downloads-and-uploads-with-microsoft-entra-id>
2. <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/download-vhd?tabs=azure-portal#secure-downloads-and-uploads-with-microsoft-entra-id>

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.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

20.6 Ensure that Only Approved Extensions Are Installed (Manual)

Profile Applicability:

- Level 1

Description:

For added security, only install organization-approved extensions on VMs.

Rationale:

Azure virtual machine extensions are small applications that provide post-deployment configuration and automation tasks on Azure virtual machines. These extensions run with administrative privileges and could potentially access anything on a virtual machine. The Azure Portal and community provide several such extensions. Each organization should carefully evaluate these extensions and ensure that only those that are approved for use are actually implemented.

Impact:

Functionality by unsupported extensions will be disabled.

Audit:

Audit from Azure Portal

1. Go to **Virtual machines**.
2. For each virtual machine, click on the server name to select it.
3. In the new column menu, under **Settings** Click on **Extensions + applications**.
4. Ensure that all the listed extensions are approved by your organization for use.

Audit from Azure CLI

Use the below command to list the extensions attached to a VM, and ensure the listed extensions are approved for use.

```
az vm extension list --vm-name <vmName> --resource-group <sourceGroupName> --query [*].name
```

Audit from PowerShell

Get a list of VMs.

```
Get-AzVM
```

For each VM run the following command.

```
Get-AzVMExtension -ResourceGroupName <VM Resource Group> -VMName <VM Name>
```

Review each **Name**, **ExtensionType**, and **ProvisioningState** to make sure no unauthorized extensions are installed on any virtual machines.

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:** [c0e996f8-39cf-4af9-9f45-83fbde810432](#) - **Name:** 'Only approved VM extensions should be installed'

Remediation:

Remediate from Azure Portal

1. Go to **Virtual machines**.
2. For each virtual machine, go to **Settings**.
3. Click on **Extensions + applications**.
4. If there are unapproved extensions, uninstall them.

Remediate from Azure CLI

From the audit command identify the unapproved extensions, and use the below CLI command to remove an unapproved extension attached to VM.

```
az vm extension delete --resource-group <resourceGroupName> --vm-name  
<vmName> --name <extensionName>
```

Remediate from PowerShell

For each VM and each insecure extension from the Audit Procedure run the following command.

```
Remove-AzVMExtension -ResourceGroupName <ResourceGroupName> -Name  
<ExtensionName> -VMName <VirtualMachineName>
```







Default Value:

By default, no extensions are added to the virtual machines.

References:

1. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/extensions-features>
2. <https://docs.microsoft.com/en-us/powershell/module/az.compute/?view=azps-7.5.0#vm-extensions>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-asset-management#am-2-use-only-approved-services>
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-asset-management#am-5-use-only-approved-applications-in-virtual-machine>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.1 <u>Establish and Maintain a Software Inventory</u> Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.			
v7	2.1 <u>Maintain Inventory of Authorized Software</u> Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.			

20.7 Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)

Profile Applicability:

- Level 2

Description:

Install endpoint protection for all virtual machines.

Rationale:

Installing endpoint protection systems (like anti-malware for Azure) provides for real-time protection capability that helps identify and remove viruses, spyware, and other malicious software. These also offer configurable alerts when known-malicious or unwanted software attempts to install itself or run on Azure systems.

Impact:

Endpoint protection will incur an additional cost to you.

Audit:

Audit from Azure Portal

1. Go to **Security Center**
2. Click the **Recommendations** blade
3. Ensure that there are no recommendations for **Endpoint Protection not installed on Azure VMs**

Audit from Azure CLI

```
az vm show -g <MyResourceGroup> -n <MyVm> -d --query  
"resources[?type=='Microsoft.Compute/virtualMachines/extensions'].{ExtensionName:name}" -o table
```

If extensions are installed, it will list the installed extensions.

```
EndpointSecurity || TrendMicroDSA* || Antimalware || EndpointProtection ||  
SCWPAgent || PortalProtectExtension* || FileSecurity*
```

Alternatively, you can employ your own endpoint protection tool 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:** [501541f7-f7e7-4cd6-868c-4190fdad3ac9](#) - **Name:** 'A vulnerability assessment solution should be enabled on your virtual machines'

Remediation:

Follow Microsoft Azure documentation to install endpoint protection from the security center. Alternatively, you can employ your own endpoint protection tool for your OS.







Default Value:

By default Endpoint Protection is disabled.

References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-install-endpoint-protection>
2. <https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware>
3. https://docs.microsoft.com/en-us/cli/azure/vm/extension?view=azure-cli-latest#az_vm_extension_list
4. <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	10.2 <u>Configure Automatic Anti-Malware Signature Updates</u> Configure automatic updates for anti-malware signature files on all enterprise assets.			
v7	8.2 <u>Ensure Anti-Malware Software and Signatures are Updated</u> Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.			

20.8 [Legacy] Ensure that VHDs are Encrypted (Manual)

Profile Applicability:

- Level 2

Description:

NOTE: This is a legacy recommendation. Managed Disks are encrypted by default and recommended for all new VM implementations.

VHD (Virtual Hard Disks) are stored in blob storage and are the old-style disks that were attached to Virtual Machines. The blob VHD was then leased to the VM. By default, storage accounts are not encrypted, and Microsoft Defender will then recommend that the OS disks should be encrypted. Storage accounts can be encrypted as a whole using PMK or CMK. This should be turned on for storage accounts containing VHDs.

Rationale:

While it is recommended to use Managed Disks which are encrypted by default, "legacy" VHDs may exist for a variety of reasons and may need to remain in VHD format. VHDs are not encrypted by default, so this recommendation intends to address the security of these disks. In these niche cases, VHDs should be encrypted using the procedures in this recommendation to encrypt and protect the data content.

If a virtual machine is using a VHD and can be converted to a managed disk, instructions for this procedure can be found in the resources section of this recommendation under the title "Convert VHD to Managed Disk."

Impact:

Depending on how the encryption is implemented will change the size of the impact. If provider-managed keys(PMK) are utilized, the impact is relatively low, but processes need to be put in place to regularly rotate the keys. If Customer-managed keys(CMK) are utilized, a key management process needs to be implemented to store and manage key rotation, thus the impact is medium to high depending on user maturity with key management.

Audit:

Audit from Azure CLI

For each virtual machine identify if the VM is using a legacy VHD by reviewing the *VHD* parameter in the output of the following command. The *VHD* parameter will contain the Storage Account name used for the VHD.

```
az vm show --name <MyVM> --resource-group <MyResourceGroup>
```

Next, identify if the storage account from the *VHD* parameter is encrypted by reviewing the *encryption --> services --> blob --> enabled* within the output of the following command and make sure its value is *True*.

```
az storage account show --name <storage account name> --resource-group <resource group>
```

Audit from PowerShell:

Determine whether the VM is using a VHD for the OS Disk and any Data disks.

```
$virtualMachine = Get-AzVM --Name <vm name> --ResourceGroup <resource group name> |Select-Object -ExpandProperty StorageProfile  
  
$virtualMachine.OsDisk  
$virtualMachine.DataDisks
```

Next, use the value from *VHD* to see if the storage blob holding the VHD is encrypted.

```
$storageAccount = Get-AzStorageAccount -Name <storage account name from VHD setting> -ResourceGroupName <resource group name>  
  
$storageAccount.Encryption.Services.Blob
```

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:** [702dd420-7fcc-42c5-afe8-4026edd20fe0](#) - **Name:** 'OS and data disks should be encrypted with a customer-managed key'

Remediation:

Remediate from Azure Portal

1. Navigate to the **storage account** that you wish to encrypt
2. Select **encryption**
3. Select the **encryption type** that you wish to use

If you wish to use a Microsoft-managed key (the default), you can save at this point and encryption will be applied to the account.

If you select **Customer-managed keys**, it will ask for the location of the key (The default is an Azure Key Vault) and the key name.

Once these are captured, save the configuration and the account will be encrypted using the provided key.

Remediate from Azure CLI:

Create the Key Vault

```
az keyvault create --name <name> --resource-group <resourceGroup> --location <location> --enabled-for-disk-encryption
```

Encrypt the disk and store the key in Key Vault

```
az vm encryption enable -g <resourceGroup> --name <name> --disk-encryption-keyvault myKV
```

Remediate from PowerShell

This process uses a Key Vault to store the keys

Create the Key Vault

```
New-AzKeyvault -name <name> -ResourceGroupName <resourceGroup> -Location  
<location> -EnabledForDiskEncryption
```

Encrypt the disk and store the key in Key Vault

```
$KeyVault = Get-AzKeyVault -VaultName <name> -ResourceGroupName  
<resourceGroup>  
Set-AzVMDiskEncryptionExtension -ResourceGroupName <resourceGroup> -VMName  
<name> -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -  
DiskEncryptionKeyVaultId $KeyVault.ResourceId
```

Default Value:

The default value for encryption is "NO Encryption"

References:

1. CLI: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-cli-quickstart>
2. Powershell: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-powershell-quickstart>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default>
4. Convert VHD to Managed Disk: <https://docs.microsoft.com/en-us/previous-versions/azure/virtual-machines/scripts/virtual-machines-powershell-sample-create-managed-disk-from-vhd>

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.			●

20.9 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 least privileges principal

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 that are provisioned to a virtual machine utilizes an RBAC/ABAC group and is allocated a role using Azure PIM, and 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**:
 1. Under **Manage**, click **Users**.

2. Click **Per-user MFA**.
3. 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**:
 1. Under **Manage**, click **Security**.
 2. Under **Protect**, click **Conditional Access**.
 3. 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**:
 1. Under **Manage**, click **Users**.
 2. Click **Per-user MFA**.
 3. For each user requiring remediation, check the box next to their name.
 4. Click **Enable MFA**.
 5. Click **Enable**.
 3. For **Conditional Access**:
 1. Under **Manage**, click **Security**.
 2. Under **Protect**, click **Conditional Access**.
 3. 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 <u>Require MFA for Administrative Access</u> 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 <u>Use Multifactor Authentication For All Administrative Access</u> Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

20.10 Ensure Trusted Launch is enabled on Virtual Machines (Automated)

Profile Applicability:

- Level 1

Description:

When **Secure Boot** and **vTPM** are enabled together, they provide a strong foundation for protecting your VM from boot attacks. For example, if an attacker attempts to replace the bootloader with a malicious version, Secure Boot will prevent the VM from booting. If the attacker is able to bypass Secure Boot and install a malicious bootloader, vTPM can be used to detect the intrusion and alert you.

Rationale:

Secure Boot and vTPM work together to protect your VM from a variety of boot attacks, including bootkits, rootkits, and firmware rootkits. Not enabling Trusted Launch in Azure VM can lead to increased vulnerability to rootkits and boot-level malware, reduced ability to detect and prevent unauthorized changes to the boot process, and a potential compromise of system integrity and data security.

Impact:

Secure Boot and vTPM are not currently supported for Azure Generation 1 VMs.

IMPORTANT: Before enabling Secure Boot and vTPM on a Generation 2 VM which does not already have both enabled, it is highly recommended to create a restore point of the VM prior to remediation.

Audit:

Audit from Azure Portal

1. Go to Virtual Machines
2. For each VM, under Settings, click on Configuration on the left blade
3. Under Security Type, make sure security type is not standard and if it is Trusted Launch Virtual Machines then make sure Enable Secure Boot & Enable vTPM are checked

Audit from Azure CLI

Run the following command to list VM names and security profile settings:

```
az vm list --query [*].[name,securityProfile]
```

For each VM, ensure that **securityType** is set to **TrustedLaunch**, **uefiSettings.secureBootEnabled** is set to **true**, and **uefiSettings.vTpmEnabled** is set to **true**.

Audit from PowerShell

Run the following command to list VMs:

```
Get-AzVm
```

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

```
$vm = Get-AzVm -ResourceGroupName <resource-group> -Name <vm>
```

Run the following command to get the security profile settings for the VM:

```
$vm.SecurityProfile
```

Ensure that **SecurityType** is set to **TrustedLaunch**.

Run the following command to get the UEFI settings for the VM:

```
$vm.SecurityProfile.UefiSettings
```

Ensure that **SecureBootEnabled** and **VTpmEnabled** are set to **True**.

Repeat for each VM.

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:** [c95b54ad-0614-4633-ab29-104b01235cbf](#) - **Name:** 'Virtual Machine should have TrustedLaunch enabled'

Remediation:

Note: Trusted launch on existing virtual machines (VMs) is currently not supported for Azure Generation 1 VMs

Remediate from Azure Portal

1. Go to Virtual Machines.
2. For each VM, under Settings, click on Configuration on the left blade.
3. Under Security Type, select 'Trusted Launch Virtual Machines'.
4. Make sure Enable Secure Boot & Enable vTPM are checked.
5. Click on Apply.

Remediate from Azure CLI

Ensure that it is safe to change the state of the VM.

Run the following command to deallocate the VM:

```
az vm deallocate --resource-group <resource-group> --name <vm>
```

Run the following command to update the VM, setting security type to **TrustedLaunch** and enabling **secure boot** and **vTPM**:


```
az vm update --resource-group <resource-group> --name <vm> --enable-secure-boot true --enable-vtpm true --security-type TrustedLaunch
```

Run the following command to restart the VM:

```
az vm start --resource-group <resource-group> --name <vm>
```

Repeat for each VM requiring remediation.

Remediate from PowerShell

Ensure that it is safe to change the state of the VM.

Run the following command to stop the VM:

```
Stop-AzVm -ResourceGroupName <resource-group> -Name <vm> -Force
```

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

```
$vm = Get-AzVM -ResourceGroupName <resource-group> -Name <vm>
```

Run the following command to update the VM, setting security type to **TrustedLaunch** and enabling **secure boot** and **vTPM**:

```
Update-AzVm -ResourceGroupName <resource-group> -VM $vm -EnableSecureBoot 1 -EnableVtpm 1 -SecurityType TrustedLaunch
```

Run the following command to start the VM:

```
Start-AzVm -ResourceGroupName <resource-group> -Name <vm>
```

Repeat for each VM requiring remediation.







Default Value:

On Azure Generation 2 VMs, vTPM is enabled by default. Secure Boot is not enabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch-existing-vm?tabs=portal>
2. <https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch-existing-vm?tabs=portal#enable-trusted-launch-on-existing-vm>
3. <https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch#secure-boot>
4. <https://learn.microsoft.com/en-us/cli/azure/vm>
5. <https://learn.microsoft.com/en-us/powershell/module/az.compute/get-azvm>
6. <https://learn.microsoft.com/en-us/powershell/module/az.compute/stop-azvm>
7. <https://learn.microsoft.com/en-us/powershell/module/az.compute/update-azvm>
8. <https://learn.microsoft.com/en-us/powershell/module/az.compute/start-azvm>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

20.11 Ensure that encryption at host is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Encryption at host enhances Azure Disk Storage Server-Side Encryption to ensure that all temporary disks and disk caches are encrypted at rest and flow encrypted to the storage clusters.

Rationale:

Encryption at host provides an additional layer of security to protect sensitive information.

Impact:

- Virtual machines must be deallocated for encryption at host to be enabled.
- Encryption at host does not use virtual machine CPU, and does not impact virtual machine performance.
- Encryption at host cannot be enabled on virtual machines that have ever had Azure Disk Encryption enabled.

Audit:

Audit from Azure Portal

1. Go to **Virtual machines**.
2. Click the name of a virtual machine.
3. In the **Properties** pane, under **Disk**, ensure that **Encryption at host** is set to **Enabled**.
4. Repeat steps 1-3 for each virtual machine.

Audit from Azure CLI

Run the following command to list VM names and security profile settings:

```
az vm list --query [*].name,securityProfile
```

For each VM, ensure that **encryptionAtHost** is set to **true**.

Audit from PowerShell

Run the following command to list VMs:

```
Get-AzVm
```

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

```
$vm = Get-AzVm -ResourceGroupName <resource-group> -Name <vm>
```

Run the following command to get the security profile settings for the VM:

```
$vm.SecurityProfile
```

Ensure that **EncryptionAtHost** is set to **True**.
Repeat for each VM.

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:** [fc4d8e41-e223-45ea-9bf5-eada37891d87](#) - **Name:** 'Virtual machines and virtual machine scale sets should have encryption at host enabled'

Remediation:

Note: Encryption at host must first be enabled in a subscription before it can be used for virtual machines.

1. From Azure Portal, select the Cloud Shell icon.
2. Run the following command to set the context to the current subscription:

```
Set-AzContext -SubscriptionId <subscription-id>
```

1. Run the following command to register the encryption at host feature for the subscription:

```
Register-AzProviderFeature -FeatureName "EncryptionAtHost" -ProviderNamespace "Microsoft.Compute"
```

1. Run the following command to confirm that the **RegistrationState** is **Registered**:

```
Get-AzProviderFeature -FeatureName "EncryptionAtHost" -ProviderNamespace "Microsoft.Compute"
```

Remediate from Azure Portal

Note: Ensure that it is safe to change the state of the VM.

1. Go to **Virtual machines**.
2. Click the name of a virtual machine.
3. Click **Stop**.
4. Click **Yes**.
5. Under **Settings**, click **Disks**.
6. Click **Additional settings**.
7. Next to **Encryption at host**, select **Yes**.

8. Click **Save**.
9. Click **Overview**.
10. Click **Start**.
11. Repeat steps 1-10 for each virtual machine requiring remediation.

Remediate from Azure CLI

Note: Ensure that it is safe to change the state of the VM.

Run the following command to deallocate the VM:

```
az vm deallocate --resource-group <resource-group> --name <vm>
```

Run the following command to update the VM, enabling **encryptionAtHost**:

```
az vm update --resource-group <resource-group> --name <vm> --set securityProfile.encryptionAtHost=true
```

Run the following command to restart the VM:

```
az vm start --resource-group <resource-group> --name <vm>
```

Repeat for each VM requiring remediation.

Remediate from PowerShell

Note: Ensure that it is safe to change the state of the VM.

Run the following command to stop the VM:

```
Stop-AzVm -ResourceGroupName <resource-group> -Name <vm> -Force
```

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

```
$vm = Get-AzVM -ResourceGroupName <resource-group> -Name <vm>
```

Run the following command to update the VM, enabling **encryptionAtHost**:

```
Update-AzVm -ResourceGroupName <resource-group> -VM $vm -EncryptionAtHost 1
```

Run the following command to start the VM:

```
Start-AzVm -ResourceGroupName <resource-group> -Name <vm>
```

Repeat for each VM requiring remediation.

Default Value:








Encryption at host is disabled by default.

References:

1. <https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview>
2. <https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption#encryption-at-host---end-to-end-encryption-for-your-vm-data>
3. <https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal>

4. <https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disks-enable-host-based-encryption-cli>
5. <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-host-based-encryption-powershell>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Introduction		
1.1	CIS Microsoft Azure Foundations Benchmarks		
1.2	CIS Microsoft Azure Service Category Benchmarks		
1.3	Multiple Methods of Audit and Remediation		
2	App Service		
2.1	App Service Apps		
2.1.1	Ensure 'Java version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure 'Python version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure 'PHP version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure 'FTP State' is set to 'FTPS only' or 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure 'HTTPS Only' is set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure end-to-end TLS encryption is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure 'Remote debugging' is set to 'Off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.11	Ensure incoming client certificates are enabled and required (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure 'App Service authentication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure managed identities are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure public network access is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure App Service plan SKU supports private endpoints (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure private endpoints are used to access App Service apps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure private endpoints used to access App Service apps use private DNS zones (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure app is integrated with a virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure configuration is routed through the virtual network integration (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure all traffic is routed through the virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure cross-origin resource sharing does not allow all origins (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	App Service Deployment Slots		
2.2.1	Ensure 'Java version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure 'Python version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure 'PHP version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure 'HTTPS Only' is set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure end-to-end TLS encryption is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure 'Remote debugging' is set to 'Off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure incoming client certificates are enabled and required (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure managed identities are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure public network access is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure deployment slot is integrated with a virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure configuration is routed through the virtual network integration (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure all traffic is routed through the virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure cross-origin resource sharing does not allow all origins (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Function Apps		
2.3.1	Ensure 'Java version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.2	Ensure 'Python version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure 'HTTPS Only' is set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure end-to-end TLS encryption is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9	Ensure 'Remote debugging' is set to 'Off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10	Ensure incoming client certificates are enabled and required (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Ensure 'App Service authentication' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.12	Ensure managed identities are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.13	Ensure public network access is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.14	Ensure function app is integrated with a virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.15	Ensure configuration is routed through the virtual network integration (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.16	Ensure all traffic is routed through the virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3.17	Ensure cross-origin resource sharing does not allow all origins (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Functions Deployment Slots		
2.4.1	Ensure 'Java version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure 'Python version' is currently supported (if in use) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure 'HTTP version' is set to '2.0' (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.6	Ensure 'HTTPS Only' is set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.8	Ensure end-to-end TLS encryption is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.9	Ensure 'Remote debugging' is set to 'Off' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure incoming client certificates are enabled and required (if in use) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.11	Ensure managed identities are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure public network access is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.13	Ensure deployment slot is integrated with a virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.14	Ensure configuration is routed through the virtual network integration (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4.15	Ensure all traffic is routed through the virtual network (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.16	Ensure cross-origin resource sharing does not allow all origins (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Azure Key Vaults are Used to Store Secrets (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure App Service Environment is deployed with an internal load balancer (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure App Service Environment is provisioned with v3 or higher (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure App Service Environment has internal encryption enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure App Service Environment has TLS 1.0 and 1.1 disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure App Service Environment has TLS cipher suite ordering configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3	Azure Container Instances		
3.1	Ensure Private Virtual Networks are used for Container Instances (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure a Managed Identity is used for interactions with other Azure services (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure the principle of least privilege is used when assigning roles to a Managed Identity (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4	Azure CycleCloud		
4.1	Ensure SSL is configured for CycleCloud (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5	Azure Dedicated Host		
6	Azure Functions (Reference)		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7	Azure Kubernetes Service (Reference)		
8	Azure Quantum		
9	Azure Service Fabric		
10	Azure Spot Virtual Machines (Reference)		
11	Azure Spring Apps (Retiring)		
12	Azure Virtual Desktop (Reference)		
13	Azure VM Image Builder		
14	Azure VMware Solution		
15	Batch		
15.1	Ensure Batch account is set to use customer-managed keys to encrypt data (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure Batch pools disk encryption is set enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
15.3	Ensure local authentication methods for accounts are disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
15.4	Ensure Private endpoints are considered for Batch accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
15.5	Ensure public network access is disabled for Batch accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
15.6	Ensure private DNS zones for private endpoints that connect to Batch accounts are configured. (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
15.7	Ensure Diagnostics settings logs for Batch accounts are enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
16	Linux Virtual Machines (Reference)		
17	SQL Server on Azure Virtual Machines (Reference)		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18	Static Web Apps (Reference)		
19	Virtual Machine Scale Sets		
20	Virtual Machines		
20.1	Ensure Virtual Machines are utilizing Managed Disks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
20.2	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
20.3	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
20.4	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
20.5	Ensure that 'Enable Data Access Authentication Mode' is 'Checked' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
20.6	Ensure that Only Approved Extensions Are Installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
20.7	Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
20.8	[Legacy] Ensure that VHDs are Encrypted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
20.9	Ensure only MFA enabled identities can access privileged Virtual Machine (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
20.10	Ensure Trusted Launch is enabled on Virtual Machines (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
20.11	Ensure that encryption at host is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Azure Key Vaults are Used to Store Secrets	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure App Service Environment is deployed with an internal load balancer	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure App Service Environment is provisioned with v3 or higher	<input type="checkbox"/>	<input type="checkbox"/>
20.4	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	<input type="checkbox"/>	<input type="checkbox"/>
20.5	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	<input type="checkbox"/>	<input type="checkbox"/>
20.6	Ensure that Only Approved Extensions Are Installed	<input type="checkbox"/>	<input type="checkbox"/>
20.7	Ensure that Endpoint Protection for all Virtual Machines is installed	<input type="checkbox"/>	<input type="checkbox"/>
20.10	Ensure Trusted Launch is enabled on Virtual Machines	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure 'FTP State' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure App Service plan SKU supports private endpoints	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure private endpoints are used to access App Service apps	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure private endpoints used to access App Service apps use private DNS zones	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.2.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.14	Ensure function app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.3.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.4.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.11	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.13	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.14	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.4.15	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.16	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Azure Key Vaults are Used to Store Secrets	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure App Service Environment is deployed with an internal load balancer	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure App Service Environment is provisioned with v3 or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure App Service Environment has internal encryption enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure App Service Environment has TLS 1.0 and 1.1 disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure App Service Environment has TLS cipher suite ordering configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure SSL is configured for CycleCloud	<input type="checkbox"/>	<input type="checkbox"/>
15.3	Ensure local authentication methods for accounts are disabled	<input type="checkbox"/>	<input type="checkbox"/>
15.4	Ensure Private endpoints are considered for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.5	Ensure public network access is disabled for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.6	Ensure private DNS zones for private endpoints that connect to Batch accounts are configured.	<input type="checkbox"/>	<input type="checkbox"/>
15.7	Ensure Diagnostics settings logs for Batch accounts are enabled	<input type="checkbox"/>	<input type="checkbox"/>
20.4	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	<input type="checkbox"/>	<input type="checkbox"/>
20.5	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	<input type="checkbox"/>	<input type="checkbox"/>
20.6	Ensure that Only Approved Extensions Are Installed	<input type="checkbox"/>	<input type="checkbox"/>
20.7	Ensure that Endpoint Protection for all Virtual Machines is installed	<input type="checkbox"/>	<input type="checkbox"/>
20.9	Ensure only MFA enabled identities can access privileged Virtual Machine	<input type="checkbox"/>	<input type="checkbox"/>
20.10	Ensure Trusted Launch is enabled on Virtual Machines	<input type="checkbox"/>	<input type="checkbox"/>
20.11	Ensure that encryption at host is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure 'FTP State' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure App Service plan SKU supports private endpoints	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure private endpoints are used to access App Service apps	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure private endpoints used to access App Service apps use private DNS zones	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.2.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.14	Ensure function app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.3.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.4.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.11	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.13	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.14	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.4.15	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.16	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Azure Key Vaults are Used to Store Secrets	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure App Service Environment is deployed with an internal load balancer	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure App Service Environment is provisioned with v3 or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure App Service Environment has internal encryption enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure App Service Environment has TLS 1.0 and 1.1 disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure App Service Environment has TLS cipher suite ordering configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure SSL is configured for CycleCloud	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure Batch account is set to use customer-managed keys to encrypt data	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure Batch pools disk encryption is set enabled	<input type="checkbox"/>	<input type="checkbox"/>
15.3	Ensure local authentication methods for accounts are disabled	<input type="checkbox"/>	<input type="checkbox"/>
15.4	Ensure Private endpoints are considered for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.5	Ensure public network access is disabled for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.6	Ensure private DNS zones for private endpoints that connect to Batch accounts are configured.	<input type="checkbox"/>	<input type="checkbox"/>
15.7	Ensure Diagnostics settings logs for Batch accounts are enabled	<input type="checkbox"/>	<input type="checkbox"/>
20.1	Ensure Virtual Machines are utilizing Managed Disks	<input type="checkbox"/>	<input type="checkbox"/>
20.2	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
20.3	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
20.4	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	<input type="checkbox"/>	<input type="checkbox"/>
20.5	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	<input type="checkbox"/>	<input type="checkbox"/>
20.6	Ensure that Only Approved Extensions Are Installed	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
20.7	Ensure that Endpoint Protection for all Virtual Machines is installed	<input type="checkbox"/>	<input type="checkbox"/>
20.8	[Legacy] Ensure that VHDs are Encrypted	<input type="checkbox"/>	<input type="checkbox"/>
20.9	Ensure only MFA enabled identities can access privileged Virtual Machine	<input type="checkbox"/>	<input type="checkbox"/>
20.10	Ensure Trusted Launch is enabled on Virtual Machines	<input type="checkbox"/>	<input type="checkbox"/>
20.11	Ensure that encryption at host is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1	Ensure Private Virtual Networks are used for Container Instances	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure a Managed Identity is used for interactions with other Azure services	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure the principle of least privilege is used when assigning roles to a Managed Identity	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Azure Key Vaults are Used to Store Secrets	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure App Service Environment is deployed with an internal load balancer	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure App Service Environment is provisioned with v3 or higher	<input type="checkbox"/>	<input type="checkbox"/>
20.4	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	<input type="checkbox"/>	<input type="checkbox"/>
20.5	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	<input type="checkbox"/>	<input type="checkbox"/>
20.6	Ensure that Only Approved Extensions Are Installed	<input type="checkbox"/>	<input type="checkbox"/>
20.7	Ensure that Endpoint Protection for all Virtual Machines is installed	<input type="checkbox"/>	<input type="checkbox"/>
20.9	Ensure only MFA enabled identities can access privileged Virtual Machine	<input type="checkbox"/>	<input type="checkbox"/>
20.10	Ensure Trusted Launch is enabled on Virtual Machines	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure 'FTP State' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure App Service plan SKU supports private endpoints	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure private endpoints are used to access App Service apps	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure private endpoints used to access App Service apps use private DNS zones	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.2.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.14	Ensure function app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.3.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.4.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.11	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.13	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.14	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.4.15	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.16	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Azure Key Vaults are Used to Store Secrets	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure App Service Environment is deployed with an internal load balancer	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure App Service Environment is provisioned with v3 or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure App Service Environment has internal encryption enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure App Service Environment has TLS 1.0 and 1.1 disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure App Service Environment has TLS cipher suite ordering configured	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure Private Virtual Networks are used for Container Instances	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure a Managed Identity is used for interactions with other Azure services	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure the principle of least privilege is used when assigning roles to a Managed Identity	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure SSL is configured for CycleCloud	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure Batch account is set to use customer-managed keys to encrypt data	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure Batch pools disk encryption is set enabled	<input type="checkbox"/>	<input type="checkbox"/>
15.3	Ensure local authentication methods for accounts are disabled	<input type="checkbox"/>	<input type="checkbox"/>
15.4	Ensure Private endpoints are considered for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.5	Ensure public network access is disabled for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.6	Ensure private DNS zones for private endpoints that connect to Batch accounts are configured.	<input type="checkbox"/>	<input type="checkbox"/>
15.7	Ensure Diagnostics settings logs for Batch accounts are enabled	<input type="checkbox"/>	<input type="checkbox"/>
20.1	Ensure Virtual Machines are utilizing Managed Disks	<input type="checkbox"/>	<input type="checkbox"/>
20.2	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
20.3	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
20.4	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	<input type="checkbox"/>	<input type="checkbox"/>
20.5	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	<input type="checkbox"/>	<input type="checkbox"/>
20.6	Ensure that Only Approved Extensions Are Installed	<input type="checkbox"/>	<input type="checkbox"/>
20.7	Ensure that Endpoint Protection for all Virtual Machines is installed	<input type="checkbox"/>	<input type="checkbox"/>
20.8	[Legacy] Ensure that VHDs are Encrypted	<input type="checkbox"/>	<input type="checkbox"/>
20.9	Ensure only MFA enabled identities can access privileged Virtual Machine	<input type="checkbox"/>	<input type="checkbox"/>
20.10	Ensure Trusted Launch is enabled on Virtual Machines	<input type="checkbox"/>	<input type="checkbox"/>
20.11	Ensure that encryption at host is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure 'FTP State' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure App Service plan SKU supports private endpoints	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure private endpoints are used to access App Service apps	<input type="checkbox"/>	<input type="checkbox"/>
2.1.17	Ensure private endpoints used to access App Service apps use private DNS zones	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.2.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure 'PHP version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.6	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.7	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.8	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.2.9	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.10	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.2.11	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.2.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.2.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.2.14	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.2.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.2.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.3.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.3.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.3.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.3.11	Ensure 'App Service authentication' is set to 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.3.12	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3.13	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.3.14	Ensure function app is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.15	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.3.16	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.3.17	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.4.1	Ensure 'Java version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.2	Ensure 'Python version' is currently supported (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.3	Ensure 'Basic Authentication Publishing Credentials' are 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.4	Ensure 'FTP state' is set to 'FTPS only' or 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.5	Ensure 'HTTP version' is set to '2.0' (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.6	Ensure 'HTTPS Only' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.7	Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.4.8	Ensure end-to-end TLS encryption is enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.9	Ensure 'Remote debugging' is set to 'Off'	<input type="checkbox"/>	<input type="checkbox"/>
2.4.10	Ensure incoming client certificates are enabled and required (if in use)	<input type="checkbox"/>	<input type="checkbox"/>
2.4.11	Ensure managed identities are configured	<input type="checkbox"/>	<input type="checkbox"/>
2.4.12	Ensure public network access is disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.4.13	Ensure deployment slot is integrated with a virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.14	Ensure configuration is routed through the virtual network integration	<input type="checkbox"/>	<input type="checkbox"/>
2.4.15	Ensure all traffic is routed through the virtual network	<input type="checkbox"/>	<input type="checkbox"/>
2.4.16	Ensure cross-origin resource sharing does not allow all origins	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure Azure Key Vaults are Used to Store Secrets	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure App Service Environment is deployed with an internal load balancer	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Ensure App Service Environment is provisioned with v3 or higher	<input type="checkbox"/>	<input type="checkbox"/>
2.8	Ensure App Service Environment has internal encryption enabled	<input type="checkbox"/>	<input type="checkbox"/>
2.9	Ensure App Service Environment has TLS 1.0 and 1.1 disabled	<input type="checkbox"/>	<input type="checkbox"/>
2.10	Ensure App Service Environment has TLS cipher suite ordering configured	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure Private Virtual Networks are used for Container Instances	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure a Managed Identity is used for interactions with other Azure services	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure the principle of least privilege is used when assigning roles to a Managed Identity	<input type="checkbox"/>	<input type="checkbox"/>
4.1	Ensure SSL is configured for CycleCloud	<input type="checkbox"/>	<input type="checkbox"/>
15.1	Ensure Batch account is set to use customer-managed keys to encrypt data	<input type="checkbox"/>	<input type="checkbox"/>
15.2	Ensure Batch pools disk encryption is set enabled	<input type="checkbox"/>	<input type="checkbox"/>
15.3	Ensure local authentication methods for accounts are disabled	<input type="checkbox"/>	<input type="checkbox"/>
15.4	Ensure Private endpoints are considered for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.5	Ensure public network access is disabled for Batch accounts	<input type="checkbox"/>	<input type="checkbox"/>
15.6	Ensure private DNS zones for private endpoints that connect to Batch accounts are configured.	<input type="checkbox"/>	<input type="checkbox"/>
15.7	Ensure Diagnostics settings logs for Batch accounts are enabled	<input type="checkbox"/>	<input type="checkbox"/>
20.1	Ensure Virtual Machines are utilizing Managed Disks	<input type="checkbox"/>	<input type="checkbox"/>
20.2	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	<input type="checkbox"/>	<input type="checkbox"/>
20.3	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
20.4	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	<input type="checkbox"/>	<input type="checkbox"/>
20.5	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	<input type="checkbox"/>	<input type="checkbox"/>
20.6	Ensure that Only Approved Extensions Are Installed	<input type="checkbox"/>	<input type="checkbox"/>
20.7	Ensure that Endpoint Protection for all Virtual Machines is installed	<input type="checkbox"/>	<input type="checkbox"/>
20.8	[Legacy] Ensure that VHDs are Encrypted	<input type="checkbox"/>	<input type="checkbox"/>
20.9	Ensure only MFA enabled identities can access privileged Virtual Machine	<input type="checkbox"/>	<input type="checkbox"/>
20.10	Ensure Trusted Launch is enabled on Virtual Machines	<input type="checkbox"/>	<input type="checkbox"/>
20.11	Ensure that encryption at host is enabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
24-Jun-25	2.0.0	ADD - App Service - Ensure App Service Environment has internal encryption enabled (Ticket 24817)
29-May-25	2.0.0	ADD - App Service - Ensure App Service Environment has TLS 1.0 and 1.1 disabled (Ticket 24818)
12-Jun-25	2.0.0	ADD - App Service - Ensure App Service Environment has TLS cipher suite ordering configured (Ticket 24827)
13-Jun-25	2.0.0	ADD - App Service - Ensure App Service Environment is deployed with an internal load balancer (Ticket 24801)
12-Jun-25	2.0.0	ADD - App Service - Ensure App Service Environment is provisioned with v3 or higher (Ticket 24819)
10-Jun-25	2.0.0	ADD - App Service Apps - Ensure all traffic is routed through the virtual network (Ticket 24910)
10-Jun-25	2.0.0	ADD - App Service Apps - Ensure app is integrated with a virtual network (Ticket 24850)
10-Jun-25	2.0.0	ADD - App Service Apps - Ensure App Service plan SKU supports private endpoints (Ticket 25202)
29-May-25	2.0.0	ADD - App Service Apps - Ensure configuration is routed through the virtual network integration (Ticket 24838)
12-Jun-25	2.0.0	ADD - App Service Apps - Ensure cross-origin resource sharing does not allow all origins (Ticket 24880)
10-Jun-25	2.0.0	ADD - App Service Apps - Ensure end-to-end TLS encryption is enabled (Ticket 24862)
10-Jun-25	2.0.0	ADD - App Service Apps - Ensure private endpoints are used to access App Service apps (Ticket 25208)
10-Jun-25	2.0.0	ADD - App Service Apps - Ensure private endpoints used to access App Service apps use private DNS zones (Ticket 25216)

Date	Version	Changes for this version
20-Jun-25	2.0.0	ADD - App Service Apps - Ensure public network access is disabled (Ticket 24793)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure all traffic is routed through the virtual network (Ticket 24911)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Ticket 24791)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure configuration is routed through the virtual network integration (Ticket 24871)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure cross-origin resource sharing does not allow all origins (Ticket 24882)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure deployment slot is integrated with a virtual network (Ticket 24851)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure end-to-end TLS encryption is enabled (Ticket 24863)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Ticket 25152)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'HTTP version' is set to '2.0' (if in use) (Ticket 25184)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'HTTPS Only' is set to 'On' (Ticket 24803)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure incoming client certificates are enabled and required (if in use) (Ticket 24885)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'Java version' is currently supported (if in use) (Ticket 25167)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure managed identities are configured (Ticket 24835)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Ticket 25186)

Date	Version	Changes for this version
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'PHP version' is currently supported (if in use) (Ticket 25196)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure public network access is disabled (Ticket 24796)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'Python version' is currently supported (if in use) (Ticket 25170)
12-Jun-25	2.0.0	ADD - App Service Deployment Slots - Ensure 'Remote debugging' is set to 'Off' (Ticket 25158)
27-Jun-25	2.0.0	ADD - BATCH - Ensure Batch account is set to use customer-managed keys to encrypt data (Ticket 24741)
27-Jun-25	2.0.0	ADD - BATCH - Ensure Batch pools disk encryption is set to enabled (Ticket 24739)
27-Jun-25	2.0.0	ADD - BATCH - Ensure local authentication methods for accounts are disabled (Ticket 24820)
26-Jun-25	2.0.0	ADD - BATCH - Ensure private DNS zones for private endpoints that connect to Batch accounts are configured. (Ticket 24823)
27-Jun-25	2.0.0	ADD - BATCH - Ensure Private endpoints are considered for Batch accounts (Ticket 24822)
27-Jun-25	2.0.0	ADD - BATCH - Ensure public network access is disabled for Batch accounts (Ticket 24821)
26-Jun-25	2.0.0	ADD - BATCH - Ensure Resource logs in Batch accounts should be enabled (Ticket 24830)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure all traffic is routed through the virtual network (Ticket 24912)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'App Service authentication' is set to 'Enabled' (Ticket 25215)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Ticket 24873)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure configuration is routed through the virtual network integration (Ticket 24840)

Date	Version	Changes for this version
12-Jun-25	2.0.0	ADD - Function Apps - Ensure cross-origin resource sharing does not allow all origins (Ticket 24881)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure end-to-end TLS encryption is enabled (Ticket 24865)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Ticket 25153)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure function app is integrated with a virtual network (Ticket 24852)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'HTTP version' is set to '2.0' (if in use) (Ticket 25182)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'HTTPS Only' is set to 'On' (Ticket 24804)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure incoming client certificates are enabled and required (if in use) (Ticket 24904)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'Java version' is currently supported (if in use) (Ticket 25168)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure managed identities are configured (Ticket 24836)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Ticket 25188)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure public network access is disabled (Ticket 24797)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'Python version' is currently supported (if in use) (Ticket 25172)
12-Jun-25	2.0.0	ADD - Function Apps - Ensure 'Remote debugging' is set to 'Off' (Ticket 25159)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure all traffic is routed through the virtual network (Ticket 24913)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' (Ticket 24874)

Date	Version	Changes for this version
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure configuration is routed through the virtual network integration (Ticket 24872)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure cross-origin resource sharing does not allow all origins (Ticket 24883)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure deployment slot is integrated with a virtual network (Ticket 24860)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure end-to-end TLS encryption is enabled (Ticket 24866)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'FTP state' is set to 'FTPS only' or 'Disabled' (Ticket 25156)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'HTTP version' is set to '2.0' (if in use) (Ticket 25185)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'HTTPS Only' is set to 'On' (Ticket 24805)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure incoming client certificates are enabled and required (if in use) (Ticket 24906)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'Java version' is currently supported (if in use) (Ticket 25169)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure managed identities are configured (Ticket 24875)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'Minimum Inbound TLS Version' is set to '1.2' or higher (Ticket 25190)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure public network access is disabled (Ticket 24800)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'Python version' is currently supported (if in use) (Ticket 25181)
12-Jun-25	2.0.0	ADD - Functions Deployment Slots - Ensure 'Remote debugging' is set to 'Off' (Ticket 25164)

Date	Version	Changes for this version
19-May-25	2.0.0	DELETE - Ensure Private Virtual Networks are used for Container Instances - Duplicate recommendation removed (Ticket 21453)
12-Jun-25	2.0.0	UPDATE - App Service - Align Overview with Azure Benchmarks format (Ticket 24655)
12-Jun-25	2.0.0	UPDATE - App Service Apps - Ensure 'Basic Authentication Publishing Credentials' are 'Disabled' - Updates Title, Description, Rationale, and Impact Statement for accuracy and clarity (Ticket 24794)
12-Jun-25	2.0.0	UPDATE - App Service Apps - Ensure 'FTP State' is set to 'FTPS only' or 'Disabled' - Minor updates to Description and References, removes Function Apps Azure Policy from Audit Procedure (Ticket 25150)
12-Jun-25	2.0.0	UPDATE - App Service Apps - Ensure incoming client certificates are enabled and required (if in use) - Updated impact language to clarify dissonance with HTTPS recommendation, updated control mappings (Ticket 20565)
12-Jun-25	2.0.0	UPDATE - App Service Apps - Ensure managed identities are configured - Updates Title, removes Function Apps Azure Policy (Ticket 24837)
12-Jun-25	2.0.0	UPDATE - App Service Apps - Ensure 'Remote debugging' is set to 'Off' - Removes Function Apps Azure Policy (Ticket 25157)
28-Apr-25	2.0.0	UPDATE - Azure Container Instances - Align overview with Storage Services format (Ticket 24656)
28-Apr-25	2.0.0	UPDATE - Azure CycleCloud - Align overview with Storage Services format (Ticket 24657)
28-Apr-25	2.0.0	UPDATE - Azure Functions (Reference) - Align overview with Storage Services format (Ticket 24658)
29-Apr-25	2.0.0	UPDATE - Azure Kubernetes Service (Reference) - Align overview with Storage Services format (Ticket 24659)
28-Apr-25	2.0.0	UPDATE - Azure Quantum - Align overview with Storage Services format (Ticket 24660)

Date	Version	Changes for this version
28-Apr-25	2.0.0	UPDATE - Azure Service Fabric - Align overview with Storage Services format (Ticket 24679)
28-Apr-25	2.0.0	UPDATE - Azure Spot Virtual Machines (Reference) - Align overview with Storage Services format (Ticket 24680)
28-Apr-25	2.0.0	UPDATE - Azure Spring Apps - Added retirement path details to overview (Ticket 24682)
28-Apr-25	2.0.0	UPDATE - Azure Spring Apps - Align overview with Storage Services format (Ticket 24681)
28-Apr-25	2.0.0	UPDATE - Azure Virtual Desktop - Align overview with Storage Services format (Ticket 24683)
28-Apr-25	2.0.0	UPDATE - Azure VM Image Builder - Align overview with Storage Services format (Ticket 24684)
28-Apr-25	2.0.0	UPDATE - Azure VMware Solution - Align overview with Storage Services format (Ticket 24685)
28-Apr-25	2.0.0	UPDATE - Batch - Align overview with Storage Services format (Ticket 24686)
13-Jun-25	2.0.0	UPDATE - Ensure that 'Enable Data Access Authentication Mode' is 'Checked' - Impact statement updated to cover limitations on Azure Backup and Azure Site Recovery (Ticket 23630)
19-Aug-24	2.0.0	UPDATE - Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use - Prose updated to specify enabling watch for regions in use (Ticket 21660)
28-Apr-25	2.0.0	UPDATE - Introduction - Use Introduction from Storage Services Benchmark (Ticket 24651)
28-Apr-25	2.0.0	UPDATE - Linux Virtual Machines (Reference) - Align overview with Storage Services format (Ticket 24692)
28-Apr-25	2.0.0	UPDATE - Multiple Methods of Audit and Remediation - Align with overview from Foundations Benchmark (Ticket 24653)

Date	Version	Changes for this version
28-Apr-25	2.0.0	UPDATE - SQL Server on Azure Virtual Machines (Reference) - Align overview with Storage Services format (Ticket 24693)
28-Apr-25	2.0.0	UPDATE - Static Web Apps (Reference) - Align overview with Storage Services format (Ticket 24695)
28-Apr-25	2.0.0	UPDATE - Virtual Machine Scale Sets - Align overview with Storage Services format (Ticket 24696)
28-Apr-25	2.0.0	UPDATE - Virtual Machines - Align overview with Storage Services format (Ticket 24697)
26-Jun-25	2.0.0	UPDATE - Virtual Machines - Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) - Azure Policy changed to remove deprecated policy and add replacement ids. (Ticket 25329)