CIS Microsoft Azure Compute Services Benchmark

v1.0.0 - 09-14-2023

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/

Table of Contents

Overview

All CIS 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 for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

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

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
- Cloud Services
- 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/.

Intended Audience

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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
Ian McRee
Mike Wicks
Sagar Chhatrala
Mark Weaver
Steve Johnson

Recommendations

1 Introduction

Benchmark Approach:

The suggested approach for securing your cloud environment is to start with the CIS Microsoft Azure Foundations Benchmark found here: https://www.cisecurity.org/benchmark/azure. 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 including:

- Microsoft Entra ID (Azure Active Directory)
- Microsoft Defender for Cloud
- Microsoft Azure App Service
- Microsoft Azure Database Services
- Microsoft Azure Storage Accounts
- Microsoft Azure Monitor
- Microsoft Azure Networking
- Microsoft Azure Virtual Machines

The Microsoft Azure Foundation Benchmark is what you should start with when setting up your Azure environment. It is also the foundation for which all other Azure service based 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.

After configuring your environment to the CIS Microsoft Azure Foundations Benchmark, we suggest implementing the necessary configurations for the services utilized as defined in the associated product and service level benchmarks. The CIS Microsoft Azure Compute Services Benchmark provides prescriptive guidance for configuring security options for the services within Azure's Compute category. The specific Azure Services in scope for this document 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
- Cloud Services
- Linux Virtual Machines
- SQL Server on Azure Virtual Machines
- Static Web Apps
- Virtual Machine Scale Sets
- Virtual Machines

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.

1.1 Multiple Methods of Audit and Remediation

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

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

Setting Up PowerShell and Azure CLI

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

1. Global Reader
2. Security Reader
3. Subscription Contributor

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

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

The Azure CLI tool can be installed from the following location: https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli

For PowerShell, the following cmdlets are required:

1. Azure PowerShell: https://docs.microsoft.com/en-us/powershell/azure/install-az-ps-msi?view=azps-8.2.0
2. Microsoft Graph PowerShell: https://learn.microsoft.com/en-us/powershell/microsoftgraph/get-started?view=graph-powershell-1.0
3. Azure AD PowerShell for Graph: https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-2.0
4. MS Online PowerShell: https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-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 -Subscription <subscription ID> -Tenant <Tenant ID>
Connect-MgGraph
Connect-MsolService
Connect-AzureAD
```

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

2 App Service

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

2.1 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.

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`

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`.
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`.

Remediation:

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`

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
```

From PowerShell

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

Default Value:

By default, HTTPS-only feature will be disabled when a new app is created using the command-line tool or Azure Portal console.

References:

1. https://learn.microsoft.com/en-us/azure/app-service/overview-security?source=recommendations#https-and-certificates
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit
3. 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 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

2.2 Ensure App Service Authentication is set up for apps in Azure App Service (Automated)

Profile Applicability:

- Level 2

Description:

Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching a Web Application 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 logon page. To handle the logon process, a choice from a set of identity providers can be made, or a custom authentication mechanism can be implemented.

Rationale:

By Enabling App Service 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 (Azure Active Directory, Facebook, Google, Microsoft Account, and Twitter), validation, storing and refreshing of tokens, managing the authenticated sessions and injecting identity information into request headers.

Impact:

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

Adding Authentication requirement will increase cost of App Service and require additional security components to facilitate the authentication.

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 `Authentication`
5. Ensure that `App Service authentication` set to `Enabled` (Will only appear once an Identity provider is set up/selected)

From Azure CLI
To check App Service Authentication status for an existing app, run the following command,

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

The output should return `true` if App Service authentication is set to `On`.

Remediation:

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 `Authentication`
5. If no identity providers are set up, then click `Add identity provider`
6. Choose other parameters as per your requirements and click on `Add`

From Azure CLI

To set App Service Authentication for an existing app, run the following command:

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

Note

In order to access `App Service authentication` settings for Web app using Microsoft API requires `Website contributor` permission at subscription level. A custom role can be created in place of `Website contributor` to provide more specific permission and maintain the principle of least privileged access.

Default Value:

By default, App Service Authentication is disabled when a new app is created using the command-line tool or Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/app-service-authentication-overview
2. https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#website-contributor
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management
4. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy

Additional Information:

You're not required to use App Service for authentication and authorization. Many web frameworks are bundled with security features, 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 deep understanding of security, including federation, encryption, JSON web tokens (JWT) management, grant types, and so on.

CIS Controls:

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

2.3 Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

By default, App Services can be deployed over FTP. If FTP is required for an essential deployment workflow, FTPS should be required for FTP login for all App Services.

If FTPS is not expressly required for the App, the recommended setting is `Disabled`.

Rationale:

FTP is an unencrypted network protocol that will transmit 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:

Any deployment workflows that rely on FTP or FTPs rather than the WebDeploy or HTTPs endpoints may be affected.

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`

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>,
}
```

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.

Remediation:

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`

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]
```

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 based deployment is `All allowed`

References:

1. https://docs.microsoft.com/en-us/azure/app-service/deploy-ftp
2. https://docs.microsoft.com/en-us/azure/app-service/overview-security
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit
4. https://docs.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

CIS Controls:

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

2.4 Ensure Web App is using the latest version of TLS encryption (Automated)

Profile Applicability:

- Level 1

Description:

The TLS (Transport Layer Security) protocol secures transmission of data over the internet using standard encryption technology. Encryption should be set with the latest version of TLS. App service allows TLS 1.2 by default, which is the recommended TLS level by industry standards such as PCI DSS.

Rationale:

App service currently allows the web app to set TLS versions 1.0, 1.1 and 1.2. It is highly recommended to use the latest TLS 1.2 version for web app secure connections.

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 `TLS/SSL settings`
5. Under the `Bindings` pane, ensure that `Minimum TLS Version` set to `1.2` under `Protocol Settings`

From Azure CLI

To check TLS Version for an existing app, run the following command,

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

The output should return `1.2` if TLS Version is set to `1.2` (Which is currently the latest version).

From PowerShell

List all web apps.

```
Get-AzWebApp
```

For each web app run the following command.

```
Get-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME>
|Select-Object -ExpandProperty SiteConfig
```

Make sure the `minTlsVersion` is set to at least `1.2`.

Remediation:

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 `SSL settings`
5. Under the `Bindings` pane, set `Minimum TLS Version` to `1.2` under `Protocol Settings` section

From Azure CLI

To set TLS Version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--min-tls-version 1.2
```

From PowerShell

```
Set-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> -
MinTlsVersion 1.2
```

Default Value:

By default, TLS Version feature will be set to 1.2 when a new app is created using the command-line tool or Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl#enforce-tls-versions
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-8-detect-and-disable-insecure-services-and--protocols
4. https://docs.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp?view=azps-8.1.0
5. https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/create-or-update-configuration#supportedtlsversions

CIS Controls:

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

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

2.5 Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (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 who has valid certificates can access the app.

Impact:

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

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`

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`.

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`.

Remediation:

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`

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 will be disabled when a new app is created using the command-line tool or Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-authenticate-server-and-services

CIS Controls:

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

2.6 Ensure that Register with Azure Active Directory is enabled on App Service (Automated)

Profile Applicability:

- Level 1

Description:

Managed service identity in App Service provides more security by eliminating secrets from the app, such as credentials in the connection strings. When registering with Azure Active Directory in App Service, the app will connect to other Azure services securely without the need for usernames and passwords.

Rationale:

App Service provides a highly scalable, self-patching web hosting service in Azure. It also provides a managed identity for apps, which is a turn-key solution for securing access to Azure SQL Database and other Azure services.

Audit:

From Azure Portal

1. From Azure Portal open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under the `Setting` section, Click on `Identity`
5. Under the `System assigned` pane, ensure that `Status` set to `On`

From Azure CLI

To check Register with Azure Active Directory feature status for an existing app, run the following command,

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

The output should return unique Principal ID.
If no output for the above command then Register with Azure Active Directory is not set.

From PowerShell

List the web apps.

```
Get-AzWebApp
```

For each web app run the following command.

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

Make sure the `Identity` setting contains a unique Principal ID

Remediation:

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 `Identity`
5. Under the `System assigned` pane, set `Status` to `On`

From Azure CLI

To set Register with Azure Active Directory feature for an existing app, run the following command:

```
az webapp identity assign --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME>
```

From PowerShell

To register with Azure Active Directory feature for an existing app, run the following command:

```
Set-AzWebApp -AssignIdentity $True -ResourceGroupName <resource_Group_Name> -
Name <App_Name>
```

Default Value:

By default, Managed service identity via Azure AD is disabled.

References:

1. https://docs.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-connect-msi
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-1-use-centralized-identity-and-authentication-system
3. https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/create-or-update-configuration#siteconfigresource

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.		●	●

2.7 Ensure that '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 web 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
From Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the `General settings` pane, ensure that for a `Stack` of `PHP` the `Major Version` and `Minor Version` reflect a currently supported release.

NOTE: No action is required If `PHP version` is set to `Off` as PHP is not used by your web app.

From Azure CLI
To check PHP version for an existing app, run the following command,

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

From PowerShell

```
$application = Get-AzWebApp -ResourceGroupName <resource group name> -Name
<app name>
$application.SiteConfig | select-object LinuxFXVersion, phpVersion
```

The output should return a currently supported version of PHP. Any other version of PHP would be considered a finding.
NOTE: No action is required, If the output is empty as PHP is not used by your web app.

Remediation:

From Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the `General settings` pane, ensure that for a `Stack` of `PHP` the `Major Version` and `Minor Version` reflect a currently supported release.

NOTE: No action is required If `PHP version` is set to `Off` or is set with an empty value as PHP is not used by your web app.

From Azure CLI
List the available PHP runtimes:

```
az webapp list-runtimes
```

To set latest PHP version for an existing app, run the following command:

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

From PowerShell
To set latest PHP version for an existing app, run the following command:

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

NOTE: Currently there is no way to update an existing web app `Linux FX Version` setting using PowerShell, nor is there a way to create a new web app using PowerShell that configures the PHP runtime in the `Linux FX Version` setting.

Default Value:

The version of PHP is whatever was selected upon App creation.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.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

Additional Information:

Currently supported versions can be confirmed here: https://www.php.net/supported-versions.php

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.	●	●	●

2.8 Ensure that '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 web 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/

From Azure Console

1. From Azure Home open the Portal Menu in the top left
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 Python the Major version and Minor version reflect a currently supported release

NOTE: No action is required if `Python version` is set to `Off`, as Python is not used by your web app.

From Azure CLI

To check Python version for an existing app, run the following command

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --query
"{LinuxFxVersion:linuxFxVersion,WindowsFxVersion:windowsFxVersion,PythonVersi
on:pythonVersion}
```

The output should return the a currently supported version of Python.
NOTE: No action is required if the output is empty, as Python is not used by your web app.

From PowerShell

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

Ensure the output of the above command shows a currently supported of Python.
NOTE: No action is required if the output is empty, as Python is not used by your web app.

Remediation:

From Azure Portal

1. From Azure Home open the Portal Menu in the top left
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 the Major Version and the Minor Version is set to a currently supported release.

NOTE: No action is required if `Python version` is set to `Off`, as Python is not used by your web app.

From Azure CLI

To see the list of supported runtimes:

```
az webapp list-runtimes
```

To set latest Python version for an existing app, run the following command:

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

From PowerShell

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

Default Value:

The version of Python is whatever was selected upon App creation.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.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/

Additional Information:

Currently supported versions of Python can be confirmed by going to https://devguide.python.org/versions/. The currently supported versions are given the status of "security."

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.	●	●	●

2.9 Ensure that '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 web 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 version of Java here:
https://www.oracle.com/java/technologies/java-se-support-roadmap.html
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 web app.

From Azure CLI
To check Java version for an existing app, run the following command,

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

The output should return a currently supported version of Java.

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
```

Ensure the Java version used within the application is a currently supported version.

Remediation:

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 web app.

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 version>]
```

If creating a new web 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 run time version>] [--
windows-fx-version <java run time version>]
```

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 default Java version is whatever was chosen when creating the webapp.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources
4. https://www.oracle.com/java/technologies/java-se-support-roadmap.html

Additional Information:

Currently supported versions can be confirmed here:
https://www.oracle.com/java/technologies/java-se-support-roadmap.html

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

2.10 Ensure that 'HTTP20enabled' is set to 'true' (if in use) (Automated)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of HTTP may be deprecated and no longer supported. Using a supported version of HTTP for web apps is recommended to avoid vulnerabilities from outdated protocols.

HTTP 2.0 has additional performance improvements on the head-of-line blocking problem of old HTTP version, header compression, and prioritization of requests. 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.

Rationale:

Deprecated and unsupported versions of protocols such as HTTP can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

Most modern browsers support HTTP 2.0 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 buy an App Service Certificate for your app's custom domain or bind a third party certificate.

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. Ensure that `HTTP Version` set to `2.0` version under `General settings`

NOTE: Most modern browsers support HTTP 2.0 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 buy an App Service Certificate for your app's custom domain or bind a third party certificate.

From Azure CLI
To check HTTP 2.0 version status for an existing app, run the following command,

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

The output should return `true` if HTTPS 2.0 traffic value is set to `On`.

From PowerShell

For each application, run the following command:

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

If the value of the **Http20Enabled** setting is `true`, the application is compliant. Otherwise if the value of the **Http20Enabled** setting is `false`, the application is non-compliant.

Remediation:

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. Set `HTTP version` to `2.0` under `General settings`

NOTE: Most modern browsers support HTTP 2.0 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 buy an App Service Certificate for your app's custom domain or bind a third party certificate.

From Azure CLI

To set HTTP 2.0 version for an existing app, run the following command:

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

From PowerShell

To enable HTTP 2.0 version support, run the following command:

```
Set-AzWebApp -ResourceGroupName <app resource group> -Name <app name> -
Http20Enabled $true
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources
4. https://httpwg.org/specs/

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.	●	●	●

2.11 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:

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.

From Azure CLI

To list key vaults within a subscription run the following command:

```
Get-AzKeyVault
```

To list the secrets within these key vaults run the following command:

```
Get-AzKeyVaultSecret [-VaultName] <vault name>
```

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
From Azure CLI

```
az keyvault create --name "<name>" --resource-group "<myResourceGroup>" --
location myLocation
```

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:

```
{
    //...
    "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('storageConnectionStringName')]",
                    //...
                    "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://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-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.	●	●	●

3 Azure Container Instances

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

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:

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.

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 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.		●	●

3.2 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:

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.

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 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.		●	●

3.3 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 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:

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.

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:

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.

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.			●

3.4 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:

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
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 Establish and Maintain an Inventory of Service Accounts 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.		●	●
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.			●

4 Azure CycleCloud

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

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 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

5 Azure Dedicated Host

No prescriptive guidance exists yet for Microsoft Azure Dedicated Host. If you would like to contribute security best practice guidance for Microsoft Azure Dedicated Host, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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

6 Azure Functions (Reference)

Azure Functions, while considered a different product than Azure App Service, relies on the same guidance provided by Azure App Service.

Aside from the recommendations found in the section for Azure App Service, no specific prescriptive guidance exists yet for Microsoft Azure Functions. If you would like to contribute security best practice guidance for Microsoft Azure Functions, please join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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/baselines/app-service-security-baseline
- https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts?tabs=v4

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

7 Azure Kubernetes Service (Reference)

This Microsoft Azure product - Azure Kubernetes Service (AKS) - is addressed in a separate, dedicated CIS Benchmark and Community:

- Benchmark: CIS Kubernetes Benchmarks - https://www.cisecurity.org/benchmark/kubernetes
- Community: CIS Kubernetes Community - https://workbench.cisecurity.org/communities/43

8 Azure Quantum

No prescriptive guidance exists yet for Microsoft Azure Quantum. If you would like to contribute security best practice guidance for Microsoft Azure Quantum, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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

9 Azure Service Fabric

No prescriptive guidance exists yet for Microsoft Azure Service Fabric. If you would like to contribute security best practice guidance for Microsoft Azure Service Fabric, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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

10 Azure Spot Virtual Machines (Reference)

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 the CIS Microsoft Azure Compute Services Benchmark.

11 Azure Spring Apps

No prescriptive guidance exists yet for Microsoft Azure Spring Apps. If you would like to contribute security best practice guidance for Microsoft Azure Spring Apps, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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/baselines/azure-spring-apps-security-baseline

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

12 Azure Virtual Desktop

No prescriptive guidance exists yet for Microsoft Azure VM Image Builder. If you would like to contribute security best practice guidance for Microsoft Azure VM Image Builder, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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/baselines/azure-virtual-desktop-security-baseline

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.

13 Azure VM Image Builder

No prescriptive guidance exists yet for Microsoft Azure VM Image Builder. If you would like to contribute security best practice guidance for Microsoft Azure VM Image Builder, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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

14 Azure VMware Solution

No prescriptive guidance exists yet for Microsoft Azure VMware Solution. If you would like to contribute security best practice guidance for Microsoft Azure VMware Solution, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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/baselines/azure-vmware-solution-security-baseline

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

15 Batch

No prescriptive guidance exists yet for Microsoft Azure Batch. If you would like to contribute security best practice guidance for Microsoft Azure Batch, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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/baselines/batch-security-baseline

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

16 Cloud Services (Retiring)

IMPORTANT NOTE: Cloud Services (classic) is now deprecated and will be retired on August 31, 2024. If you are using Cloud Services (classic), you will need to migrate your application to Cloud Services (extended support) through Azure Resource Manager before August 31, 2024. Please review Microsoft's announcement on this service retirement here: https://azure.microsoft.com/en-us/updates/cloud-services-classic-retirement-announcement/

17 Linux Virtual Machines (Reference)

Linux Virtual Machines in Azure are deployed through the Azure Virtual Machines service. Recommendations for the Azure 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.

18 SQL Server on Azure Virtual Machines (Reference)

19 Static Web Apps (Reference)

Azure Static Web Apps, while considered a different product than Azure App Service, relies on the same guidance provided by Azure App Service.

Aside from the recommendations found in the section for Azure App Service, no specific prescriptive guidance exists yet for Azure Static Web Apps. If you would like to contribute security best practice guidance for Azure Static Web Apps, please join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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/baselines/app-service-security-baseline https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts?tabs=v4 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

20 Virtual Machine Scale Sets

No prescriptive guidance exists yet for Microsoft Azure Virtual Machine Scale Sets. If you would like to contribute security best practice guidance for Microsoft Azure Virtual Machine Scale Sets, please feel free to join the CIS Microsoft Azure Community at https://workbench.cisecurity.org.

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/baselines/virtual-machine-scale-sets-security-baseline

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

21 Virtual Machines

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

21.1 Ensure an Azure Bastion Host Exists (Automated)

Profile Applicability:

- Level 2

Description:

The Azure Bastion service allows secure remote access to Azure Virtual Machines over the Internet without exposing remote access protocol ports and services directly to the Internet. The Azure Bastion service provides this access using TLS over 443/TCP, and subscribes to hardened configurations within an organization's Azure Active Directory service.

Rationale:

The Azure Bastion service allows organizations a more secure means of accessing Azure Virtual Machines over the Internet without assigning public IP addresses to those Virtual Machines. The Azure Bastion service provides Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Virtual Machines using TLS within a web browser, thus preventing organizations from opening up 3389/TCP and 22/TCP to the Internet on Azure Virtual Machines. Additional benefits of the Bastion service includes Multi-Factor Authentication, Conditional Access Policies, and any other hardening measures configured within Azure Active Directory using a central point of access.

Impact:

The Azure Bastion service incurs additional costs and requires a specific virtual network configuration. The `Standard` tier offers additional configuration options compared to the `Basic` tier and may incur additional costs for those added features.

Audit:

From Azure Portal

1. Click on `Bastions`
2. Ensure there is at least one `Bastion` host listed under the `Name` column

From Azure CLI
Note: The Azure CLI `network bastion` module is in `Preview` as of this writing

```
az network bastion list --subscription <subscription ID>
```

Ensure the output of the above command is not empty.
From PowerShell
Retrieve the `Bastion` host(s) information for a specific `Resource Group`

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

Ensure the output of the above command is not empty.

Remediation:

Remediation Procedures
From Azure Portal*

1. Click on `Bastions`
2. Select the `Subscription`
3. Select the `Resource group`
4. Type a `Name` for the new Bastion host
5. Select a `Region`
6. Choose `Standard` next to `Tier`
7. Use the slider to set the `Instance count`
8. Select the `Virtual network` or `Create new`
9. Select the `Subnet` named `AzureBastionSubnet`. Create a `Subnet` named `AzureBastionSubnet` using a `/26` CIDR range if it doesn't already exist.
10. Selct the appropriate `Public IP address` option.
11. If `Create new` is selected for the `Public IP address` option, provide a `Public IP address name`.
12. If `Use existing` is selected for `Public IP address` option, select an IP address from `Choose public IP address`
13. Click `Next: Tags >`
14. Configure the appropriate `Tags`
15. Click `Next: Advanced >`
16. Select the appropriate `Advanced` options
17. Click `Next: Review + create >`
18. Click `Create`

From Azure CLI

```
az network bastion create --location <location> --name <name of bastion host>
--public-ip-address <public IP address name or ID> --resource-group <resource
group name or ID> --vnet-name <virtual network containing subnet called
"AzureBastionSubnet"> --scale-units <integer> --sku Standard [--disable-copy-
paste true|false] [--enable-ip-connect true|false] [--enable-tunneling
true|false]
```

From PowerShell
Create the appropriate `Virtual network` settings and `Public IP Address` settings.

```
$subnetName = "AzureBastionSubnet"
$subnet = New-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix
<IP address range in CIDR notation making sure to use a /26>
$virtualNet = New-AzVirtualNetwork -Name <virtual network name> -
ResourceGroupName <resource group name> -Location <location> -AddressPrefix
<IP address range in CIDR notation> -Subnet $subnet
$publicip = New-AzPublicIpAddress -ResourceGroupName <resource group name> -
Name <public IP address name> -Location <location> -AllocationMethod Dynamic
-Sku Standard
```

Create the `Azure Bastion` service using the information within the created variables from above.

```
New-AzBastion -ResourceGroupName <resource group name> -Name <bastion name> -
PublicIpAddress $publicip -VirtualNetwork $virtualNet -Sku "Standard" -
ScaleUnit <integer>
```

Default Value:

By default, the Azure Bastion service is not configured.

References:

1. https://learn.microsoft.com/en-us/azure/bastion/bastion-overview#sku
2. https://learn.microsoft.com/en-us/powershell/module/az.network/get-azbastion?view=azps-9.2.0
3. https://learn.microsoft.com/en-us/cli/azure/network/bastion?view=azure-cli-latest

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.1 Ensure Network Infrastructure is Up-to-Date Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

21.2 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:

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

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.

Remediation:

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.
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://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-enable-data-at-rest-encryption-by-default
3. https://docs.microsoft.com/en-us/azure/virtual-machines/faq-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 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
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.			●

21.3 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:

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.

From PowerShell

```
$ResourceGroupName="yourResourceGroupName"
$DiskName="yourDiskName"

$disk=Get-AzDisk -ResourceGroupName $ResourceGroupName -DiskName $DiskName
$disk.Encryption.Type
```

Remediation:

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

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.
NOTE 2: This may differ for Linux machines as 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-vms-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://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-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 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.			●

21.4 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:

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'

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>"
  }
]
```

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 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-vms-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://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-encrypt-sensitive-data-at-rest

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.			●

21.5 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:

From Azure Portal

1. Go to `Virtual machines`.
2. For each virtual machine, click on the server name to select it go to
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.

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
```

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.

Remediation:

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.

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>
```

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://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-asset-management#am-2-use-only-approved-services
4. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-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 Establish and Maintain a Software Inventory 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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	2.1 Maintain Inventory of Authorized Software Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	●	●	●

21.6 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:

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`

From Azure CLI

```
az vm show -g MyResourceGroup -n MyVm -d
```

It should list below or any other endpoint extensions as one of the installed extensions.

```
EndpointSecurity || TrendMicroDSA* || Antimalware || EndpointProtection ||
SCWPAgent || PortalProtectExtension* || FileSecurity*
```

Alternatively, you can employ your own endpoint protection tool for your OS.

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://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security#es-1-use-endpoint-detection-and-response-edr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●

21.7 [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:

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>
```

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
```

Remediation:

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.
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
```

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://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-encrypt-sensitive-data-at-rest
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	13 Data Protection Data Protection			

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Introduction**		
1.1	**Multiple Methods of Audit and Remediation**		
2	**App Service**		
2.1	Ensure 'HTTPS Only' is set to `On` (Automated)	□	□
2.2	Ensure App Service Authentication is set up for apps in Azure App Service (Automated)	□	□
2.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' (Automated)	□	□
2.4	Ensure Web App is using the latest version of TLS encryption (Automated)	□	□
2.5	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Automated)	□	□
2.6	Ensure that Register with Azure Active Directory is enabled on App Service (Automated)	□	□
2.7	Ensure that 'PHP version' is currently supported (if in use) (Manual)	□	□
2.8	Ensure that 'Python version' is currently supported (if in use) (Manual)	□	□
2.9	Ensure that 'Java version' is currently supported (if in use) (Manual)	□	□
2.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use) (Automated)	□	□
2.11	Ensure Azure Key Vaults are Used to Store Secrets (Manual)	□	□
3	**Azure Container Instances**		

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
3.1	Ensure Private Virtual Networks are used for Container Instances (Manual)	□	□
3.2	Ensure Private Virtual Networks are used for Container Instances (Manual)	□	□
3.3	Ensure a Managed Identity is used for interactions with other Azure services (Manual)	□	□
3.4	Ensure the principle of least privilege is used when assigning roles to a Managed Identity (Manual)	□	□
4	**Azure CycleCloud**		
4.1	Ensure SSL is configured for CycleCloud (Manual)	□	□
5	**Azure Dedicated Host**		
6	**Azure Functions (Reference)**		
7	**Azure Kubernetes Service (Reference)**		
8	**Azure Quantum**		
9	**Azure Service Fabric**		
10	**Azure Spot Virtual Machines (Reference)**		
11	**Azure Spring Apps**		
12	**Azure Virtual Desktop**		
13	**Azure VM Image Builder**		
14	**Azure VMware Solution**		
15	**Batch**		
16	**Cloud Services (Retiring)**		
17	**Linux Virtual Machines (Reference)**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
18	**SQL Server on Azure Virtual Machines (Reference)**		
19	**Static Web Apps (Reference)**		
20	**Virtual Machine Scale Sets**		
21	**Virtual Machines**		
21.1	Ensure an Azure Bastion Host Exists (Automated)	□	□
21.2	Ensure Virtual Machines are utilizing Managed Disks (Automated)	□	□
21.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)	□	□
21.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)	□	□
21.5	Ensure that Only Approved Extensions Are Installed (Manual)	□	□
21.6	Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)	□	□
21.7	[Legacy] Ensure that VHDs are Encrypted (Manual)	□	□

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
2.5	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'	□	□
2.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
2.8	Ensure that 'Python version' is currently supported (if in use)	□	□
2.9	Ensure that 'Java version' is currently supported (if in use)	□	□
2.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
2.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
21.1	Ensure an Azure Bastion Host Exists	□	□
21.5	Ensure that Only Approved Extensions Are Installed	□	□
21.6	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
2.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
2.4	Ensure Web App is using the latest version of TLS encryption	□	□
2.5	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'	□	□
2.6	Ensure that Register with Azure Active Directory is enabled on App Service	□	□
2.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
2.8	Ensure that 'Python version' is currently supported (if in use)	□	□
2.9	Ensure that 'Java version' is currently supported (if in use)	□	□
2.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
2.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
4.1	Ensure SSL is configured for CycleCloud	□	□
21.1	Ensure an Azure Bastion Host Exists	□	□
21.5	Ensure that Only Approved Extensions Are Installed	□	□
21.6	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
2.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
2.4	Ensure Web App is using the latest version of TLS encryption	□	□
2.5	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'	□	□
2.6	Ensure that Register with Azure Active Directory is enabled on App Service	□	□
2.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
2.8	Ensure that 'Python version' is currently supported (if in use)	□	□
2.9	Ensure that 'Java version' is currently supported (if in use)	□	□
2.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
2.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
4.1	Ensure SSL is configured for CycleCloud	□	□
21.1	Ensure an Azure Bastion Host Exists	□	□
21.2	Ensure Virtual Machines are utilizing Managed Disks	□	□
21.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	□	□
21.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	□	□
21.5	Ensure that Only Approved Extensions Are Installed	□	□
21.6	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure 'HTTPS Only' is set to `On`	□	□
3.1	Ensure Private Virtual Networks are used for Container Instances	□	□
3.2	Ensure Private Virtual Networks are used for Container Instances	□	□
3.3	Ensure a Managed Identity is used for interactions with other Azure services	□	□
3.4	Ensure the principle of least privilege is used when assigning roles to a Managed Identity	□	□

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
2.5	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'	□	□
2.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
2.8	Ensure that 'Python version' is currently supported (if in use)	□	□
2.9	Ensure that 'Java version' is currently supported (if in use)	□	□
2.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
2.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
21.1	Ensure an Azure Bastion Host Exists	□	□
21.5	Ensure that Only Approved Extensions Are Installed	□	□
21.6	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure 'HTTPS Only' is set to `On`	□	□
2.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
2.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
2.4	Ensure Web App is using the latest version of TLS encryption	□	□
2.5	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'	□	□
2.6	Ensure that Register with Azure Active Directory is enabled on App Service	□	□
2.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
2.8	Ensure that 'Python version' is currently supported (if in use)	□	□
2.9	Ensure that 'Java version' is currently supported (if in use)	□	□
2.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
2.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
3.1	Ensure Private Virtual Networks are used for Container Instances	□	□
3.2	Ensure Private Virtual Networks are used for Container Instances	□	□
3.3	Ensure a Managed Identity is used for interactions with other Azure services	□	□
3.4	Ensure the principle of least privilege is used when assigning roles to a Managed Identity	□	□
4.1	Ensure SSL is configured for CycleCloud	□	□
21.1	Ensure an Azure Bastion Host Exists	□	□
21.2	Ensure Virtual Machines are utilizing Managed Disks	□	□

Recommendation		Set Correctly	
		Yes	No
21.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	□	□
21.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	□	□
21.5	Ensure that Only Approved Extensions Are Installed	□	□
21.6	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
21.7	[Legacy] Ensure that VHDs are Encrypted	□	□

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure 'HTTPS Only' is set to `On`	□	□
2.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
2.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
2.4	Ensure Web App is using the latest version of TLS encryption	□	□
2.5	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'	□	□
2.6	Ensure that Register with Azure Active Directory is enabled on App Service	□	□
2.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
2.8	Ensure that 'Python version' is currently supported (if in use)	□	□
2.9	Ensure that 'Java version' is currently supported (if in use)	□	□
2.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
2.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
3.1	Ensure Private Virtual Networks are used for Container Instances	□	□
3.2	Ensure Private Virtual Networks are used for Container Instances	□	□
3.3	Ensure a Managed Identity is used for interactions with other Azure services	□	□
3.4	Ensure the principle of least privilege is used when assigning roles to a Managed Identity	□	□
4.1	Ensure SSL is configured for CycleCloud	□	□
21.1	Ensure an Azure Bastion Host Exists	□	□
21.2	Ensure Virtual Machines are utilizing Managed Disks	□	□

Recommendation		Set Correctly	
		Yes	No
21.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	□	□
21.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	□	□
21.5	Ensure that Only Approved Extensions Are Installed	□	□
21.6	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
21.7	[Legacy] Ensure that VHDs are Encrypted	□	□

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8.0	□	□