CIS Benchmarks

CIS Microsoft Azure Foundations Benchmark

v1.1.0 - 02-15-2019

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

This document, CIS Microsoft Azure Foundations Security Benchmark, provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure. This guide was tested against the listed Azure services as of Feb-2018. The scope of this benchmark is to establish the foundation level of security for anyone adopting Microsoft Azure Cloud. The benchmark is, however, not an exhaustive list of all possible security configurations and architecture. You should take the benchmark as a starting point and do the required site-specific tailoring wherever needed and when it is prudent to do so.
To obtain the latest version of this guide, please visit https://www.cisecurity.org/cis-benchmarks/. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

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

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit 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 paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

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:

Contributors
Gururaj Pandurangi
Ben Layer , Tripwire, Inc
Felix Simmons
Jonathan Trull
Pravin Goyal , Pravin Goyal
Pradeep R B
Prabhu Angadi Security Content Author (Compliance | Configuration | Checklist)
Parag Patil CISSP, ISO27001LA, ECSA, CEH
Mike Wicks GCIH, GSEC, GSLC, GCFE, ECSA
Rahul Khengare
Robin Drake
Shobha H D Information security engineer

Recommendations

1 Identity and Access Management

This section covers security recommendations that to follow to set identity and access management policies on an Azure Subscription. Identity and Access Management policies are the first step towards a defense-in-depth approach to securing an Azure Cloud Platform environment.

Most of the recommendations from this section are marked as "Not Scored" because of the lack of "Azure native CLI and API support" to perform the respective audits. However, from a security posture standpoint, these recommendations are important. According to the last communication with the Microsoft Support team regarding "Azure native CLI and API support", Microsoft teams are working to enhance "Microsoft graph API" to support all these "Azure AD" functionalities. Once we get this capability through "Microsoft Graph API", we will update the involved recommendations with the respective audit and remediation steps to make them as scored.

1.1 Ensure that multi-factor authentication is enabled for all privileged users (Not Scored)

Profile Applicability:

- Level 1

Description:

Enable multi-factor authentication for all user credentials who have write access to Azure resources. These include roles like

- Service Co-Administrators
- Subscription Owners
- Contributors

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Ensure that `MULTI-FACTOR AUTH STATUS` is `Enabled` for all users who are `Service Co-Administrators` OR `Owners` OR `Contributors`.

Microsoft Graph API
For Every Subscription, For Every Tenant
Step 1: Identify Users with Administrative Access
A> List All Users Using Microsoft Graph API:

```
GET https://graph.microsoft.com/v1.0/users
```

Capture `id` and corresponding `userPrincipalName` (`$uid`, `$userPrincipalName`)
B> List all Role Definitions Using Azure management API:

```
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsoft.Authorization/roleDefinitions?api-version=2017-05-01
```

Capture Role Definition IDs/Name (`$name`) and role names (`$properties/roleName`) where `"properties/roleName"` contains (`Owner` or `*contributor` or `admin`)
C> List All Role Assignments (Mappings `$A.uid` to `$B.name`) Using Azure Management API:

```
GET
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsoft.Authorization/roleassignments?api-version=2017-10-01-preview
```

Find all administrative roles (`$B.name`) in `"Properties/roleDefinationId"` mapped with user ids (`$A.id`) in `"Properties/principalId"` where `"Properties/principalType" == "User"`
D> Now Match (`$CProperties/principalId`) with `$A.uid` and get `$A.userPrincipalName` save this as `D.userPrincipleName`
Step 2: Run MSOL Powershell command:

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

If the output contains any of the `$D.userPrincipleName`, then this recommendation is non-compliant.
Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation. Only option is MSOL

Remediation:

Follow Microsoft Azure documentation and setup multi-factor authentication in your environment.

Impact:

Users would require two forms of authentication before any action is granted. Also, this requires an overhead for managing dual forms of authentication.

Default Value:

By default, multi-factor authentication is disabled for all users.

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication
2. https://stackoverflow.com/questions/41156206/azure-active-directory-premium-mfa-attributes-via-graph-api

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

1.2 Ensure that multi-factor authentication is enabled for all non-privileged users (Not Scored)

Profile Applicability:

- Level 2

Description:

Enable multi-factor authentication for all non-privileged users.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Ensure that for all users `MULTI-FACTOR AUTH STATUS` is `Enabled`

Microsoft Graph API
For Every Subscription, For Every Tenant
Step 1: Identify Users with non-administrative Access
A> List All Users Using Microsoft Graph API:

```
GET https://graph.microsoft.com/v1.0/users
```

Capture `id` and corresponding `userPrincipalName` (`$uid`, `$userPrincipalName`)
B> List all Role Definitions Using Azure management API:

```
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsoft.Authorization/roleDefinitions?api-version=2017-05-01
```

Capture Role Definition IDs/Name (`$name`) and role names (`$properties/roleName`) where `"properties/roleName"` does NOT contain (`Owner` or `*contributor` or `admin`)
C> List All Role Assignments (Mappings `$A.uid` to `$B.name`) Using Azure Management API:

```
GET
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsoft.Authorization/roleassignments?api-version=2017-10-01-preview
```

Find all non-administrative roles (`$B.name`) in `"Properties/roleDefinationId"` mapped with user ids (`$A.id`) in `"Properties/principalId"` where `"Properties/principalType" == "User"`
D> Now Match (`$CProperties/principalId`) with `$A.uid` and get `$A.userPrincipalName` save this as `D.userPrincipleName`
Step 2: Run MSOL Powershell command:

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

If the output contains any of the `$D.userPrincipleName`, then this recommendation is non-compliant.
Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation. Only option is MSOL

Remediation:

Follow Microsoft Azure documentation and setup multi-factor authentication in your environment.

Impact:

Users would require two forms of authentication before any action is granted. Also, this requires an overhead for managing dual forms of authentication.

Default Value:

By default, multi-factor authentication is disabled for all users.

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication

Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

1.3 Ensure that there are no guest users (Scored)

Profile Applicability:

- Level 1

Description:

Do not add guest users if not needed.

Rationale:

Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account. Until you have a business need to provide guest access to any user, avoid creating guest users. Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely leading to a potential vulnerability.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Show` drop down and select `Guest users only`
5. Ensure that there are no guest users listed (`USER TYPE` = `Guest`)

Azure Command Line Interface 2.0

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

If any users are listed, then this recommendation is non-compliant.

Remediation:

Delete the "Guest" users.

Impact:

None

Default Value:

By default, no guest users are created.

References:

1. https://blogs.microsoft.com/firehose/2017/06/14/now-you-can-invite-guest-users-to-azure-analysis-services-with-azure-active-directory-b2b/

CIS Controls:

Version 7

16.8 Disable Any Unassociated Accounts

Disable any account that cannot be associated with a business process or business owner.

1.4 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Click on `service settings`
6. Ensure that `Allow users to remember multi-factor authentication on devices they trust` is not enabled

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Click on `service settings`

6. Disable `Allow users to remember multi-factor authentication on devices they trust`

Impact:

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

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-whats-next#remember-multi-factor-authentication-for-devices-that-users-trust

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

1.5 Ensure that 'Number of methods required to reset' is set to '2' (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Like multi-factor authentication, setting up dual identification before allowing a password reset ensures that the user identity is confirmed via two separate forms of identification. With dual identification set, an attacker would require compromising both the identity forms before he/she could maliciously reset a user's password.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Authentication methods`
5. Ensure that `Number of methods required to reset` is set to `2`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Authentication methods`
5. Set the `Number of methods required to reset` to `2`

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-faq#password-reset-registration

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

1.6 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to "0" (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

If authentication re-confirmation is disabled, registered users will never be prompted to re-confirm their existing authentication information. If the authentication information for a user, such as a phone number or email changes, then the password reset information for that user reverts to the previously registered authentication information.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Registration`
5. Ensure that `Number of days before users are asked to re-confirm their authentication information` is not set to `0`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Registration`
5. Set the `Number of days before users are asked to re-confirm their authentication information` to your organization defined frequency

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#registration

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.7 Ensure that 'Notify users on password resets?' is set to 'Yes' (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Notification`
5. Ensure that `Notify users on password resets?` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Notification`
5. Set `Notify users on password resets?` to `Yes`

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#notifications

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.8 Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Notification`
5. Ensure that `notify all admins when other admins reset their password?` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Password reset`
4. Go to `Notification`
5. Set `Notify all admins when other admins reset their password?` to `Yes`

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#notifications

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

1.9 Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Require administrators to provide consent for the apps before use.

Rationale:

Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of the cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Ensure that `Users can consent to apps accessing company data on their behalf` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Set `Users can consent to apps accessing company data on their behalf` to `No`

Impact:

It might be an additional request that administrators need to fulfill quite often.

Default Value:

By default, 'Users can consent to apps accessing company data on their behalf' is set to 'Yes'.

References:

1. https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/
2. https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.10 Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Require administrators to provide consent for the apps before use.

Rationale:

Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of your cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Ensure that `Users can add gallery apps to their Access Panel` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Set `Users can add gallery apps to their Access Panel` to `No`

Impact:

It might be an additional request that administrators need to fulfill quite often.

Default Value:

By default, 'Users can add gallery apps to their Access Panel' is set to 'No'.

References:

1. https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/
2. https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx

CIS Controls:

Version 7

2 Inventory and Control of Software Assets
Inventory and Control of Software Assets

1.11 Ensure that 'Users can register applications' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Require administrators to register third-party applications.

Rationale:

It is recommended to let administrator register custom-developed applications. This ensures that the application undergoes a security review before exposing active directory data to it.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Ensure that `Users can register applications` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Set `Users can register applications` to `No`

Impact:

It might be an additional request that administrators need to fulfill quite often.

Default Value:

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

References:

1. https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/
2. https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx

CIS Controls:

Version 7

2 Inventory and Control of Software Assets
Inventory and Control of Software Assets

1.12 Ensure that 'Guest user permissions are limited' is set to 'Yes' (Not Scored)

Profile Applicability:

- Level 2

Description:

Limit guest user permissions.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Ensure that `Guest users permissions are limited` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Set `Guest users permissions are limited` to `Yes`

Impact:

None

Default Value:

By default, `Guest users permissions are limited` is set to `Yes`.

References:

1. https://blogs.microsoft.com/firehose/2017/06/14/now-you-can-invite-guest-users-to-azure-analysis-services-with-azure-active-directory-b2b/

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.13 Ensure that 'Members can invite' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Restrict invitations to administrators only.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Ensure that `Members can invite` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Set `Members can invite` to `No`

Impact:

None

Default Value:

By default, `Members can invite` is set to `Yes`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

1.14 Ensure that 'Guests can invite' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Restrict guest invitations.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Ensure that `Guests can invite` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Set `Guests can invite` to `No`

Impact:

None

Default Value:

By default, `Guests can invite` is set to `Yes`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

16 Account Monitoring and Control
Account Monitoring and Control

1.15 Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes' (Not Scored)

Profile Applicability:

- Level 1

Description:

Restrict access to the Azure AD administration portal to administrators only.

Rationale:

The Azure AD administrative portal has sensitive data. All non-administrators should be prohibited from accessing any Azure AD data in the administration portal to avoid exposure.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Ensure that `Restrict access to Azure AD administration portal` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `User settings`
4. Set `Restrict access to Azure AD administration portal` to `Yes`

Impact:

None

Default Value:

By default, `Restrict access to Azure AD administration portal` is set to `No`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles-azure-portal

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

1.16 Ensure that 'Self-service group management enabled' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Restrict group creation to administrators only.

Rationale:

Self-service group management enables users to create and manage security groups or Office 365 groups in Azure Active Directory (Azure AD). Unless a business requires this day-to-day delegation for some users, self-service group management should be disabled.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Ensure that `Self-service group management enabled` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Set `Self-service group management enabled` to `No`

Impact:

None

Default Value:

By default, `Self-service group management enabled` is set to `No`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.17 Ensure that 'Users can create security groups' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Restrict security group creation to administrators only.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Ensure that `Users can create security groups` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Set `Users can create security groups` to `No`

Impact:

None

Default Value:

By default, `Users can create security groups` is set to `No`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management#making-a-group-available-for-end-user-self-service

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.18 Ensure that 'Users who can manage security groups' is set to 'None' (Not Scored)

Profile Applicability:

- Level 2

Description:

Restrict security group management to administrators only.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Ensure that `Users who can manage security groups` is set to `None`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Set `Users who can manage security groups` to `None`

Impact:

None

Default Value:

By default, `Users who can manage security groups` is set to `All`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management#making-a-group-available-for-end-user-self-service

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.19 Ensure that 'Users can create Office 365 groups' is set to 'No' (Not Scored)

Profile Applicability:

- Level 2

Description:

Restrict Office 365 group creation to administrators only.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Ensure that `Users can create Office 365 groups` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Set `Users can create Office 365 groups` to `No`

Impact:

None

Default Value:

By default, `Users can create Office 365 groups` is set to `No`.

References:

1. https://whitepages.unlimitedviz.com/2017/01/disable-office-365-groups-2/
2. https://support.office.com/en-us/article/Control-who-can-create-Office-365-Groups-4c46c8cb-17d0-44b5-9776-005fced8e618

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.20 Ensure that 'Users who can manage Office 365 groups' is set to 'None' (Not Scored)

Profile Applicability:

- Level 2

Description:

Restrict Office 365 group management to administrators only.

Rationale:

Restricting Office 365 group management to administrators prohibits users from making changes to Office 365 groups. This ensures that Office 365 groups are appropriately managed and their management is not delegated to any other user.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Ensure that `Users who can manage Office 365 groups` is set to `None`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Set `Users who can manage Office 365 groups` to `None`

Impact:

None

Default Value:

By default, `Users who can manage Office 365 groups` to `All`.

References:

1. https://whitepages.unlimitedviz.com/2017/01/disable-office-365-groups-2/
2. https://support.office.com/en-us/article/Control-who-can-create-Office-365-Groups-4c46c8cb-17d0-44b5-9776-005fced8e618

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.21 Ensure that 'Enable "All Users" group' is set to 'Yes' (Not Scored)

Profile Applicability:

- Level 1

Description:

Enable `All Users` group for centralized administration of all users.

Rationale:

The `All Users` group can be used to assign the same permissions to all the users in the directory. For example, all users in a directory can be given access to a SaaS application by assigning access for the All Users dedicated group to this application. This ensures that there is a common policy created for all users and there is no need to restrict individual permissions.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Ensure that `Enable "All Users" group` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Group settings`
4. Set `Enable "All Users" group` to `Yes`

Impact:

None

Default Value:

By default, `Enable "All Users" group` is set to `No`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-dedicated-groups

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

1.22 Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' (Not Scored)

Profile Applicability:

- Level 1

Description:

Joining devices to the active directory should require Multi-factor authentication.

Rationale:

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

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Device settings`
4. Ensure that `Require Multi-Factor Auth to join devices` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `Device settings`
4. Set `Require Multi-Factor Auth to join devices` to `Yes`

Impact:

None

Default Value:

By default, `Require Multi-Factor Auth to join devices` is set to `No`.

References:

1. https://blogs.technet.microsoft.com/janketil/2016/02/29/azure-mfa-for-enrollment-in-intune-and-azure-ad-device-registration-explained/

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication

Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

1.23 Ensure that no custom subscription owner roles are created (Scored)

Profile Applicability:

- Level 2

Description:

Subscription ownership should not include permission to create custom owner roles. The principle of least privilege should be followed and only necessary privileges should be assigned instead of allowing full administrative access.

Rationale:

Classic subscription admin roles offer basic access management and include Account Administrator, Service Administrator, and Co-Administrators. It is recommended the least necessary permissions be given initially. Permissions can be added as needed by the account holder. This ensures the account holder cannot perform actions which were not intended.

Audit:

Azure Command Line Interface 2.0

```
az role definition list
```

Check for entries with `assignableScope` of `/` or a `subscription`, and an action of `*`
Verify the usage and impact of removing the role identified

Remediation:

Azure Command Line Interface 2.0

```
az role definition list
```

Check for entries with `assignableScope` of `/` or a `subscription`, and an action of `*`
Verify the usage and impact of removing the role identified

```
az role definition delete --name "rolename"
```

Impact:

None

Default Value:

By default, no custom owner roles are created.

References:

1. https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

16 Account Monitoring and Control
Account Monitoring and Control

2 Security Center

This section covers security recommendations to follow when setting various security policies on an Azure Subscription. A security policy defines the set of controls, which are recommended for resources within the specified Azure subscription. Please note that the majority of the recommendations mentioned in this section only produce an alert if a security violation is found. They do not actually enforce security settings by themselves. Alerts should be acted upon and remedied wherever possible.

2.1 Ensure that standard pricing tier is selected (Scored)

Profile Applicability:

- Level 2

Description:

The standard pricing tier enables threat detection for networks and virtual machines, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

Enabling the Standard pricing tier allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Audit:

Azure Console

1. Go to `Azure Security Center`
2. Select `Security policy` blade
3. Select each subscription and Click On "Edit settings"
4. Select the `Pricing tier` blade
5. Review the chosen pricing tier

Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json" GET
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/pr
icings?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.pricingTier'
```

Remediation:

Azure Console

1. Go to `Azure Security Center`
2. Select `Security policy` blade
3. Click On `Edit Settings` to alter the the security policy for a subscription
4. Select the `Pricing tier` blade

5. Select `Standard`
6. Select `Save`

Azure Command Line Interface 2.0

Use the below command to set Pricing Tier to Standard.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/pr
icings/default?api-version=2017-08-01-preview -d@"input.json"'
```

Where input.json contains the Request body json data as mentioned below.

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
default",
  "name": "default",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Impact:

Choosing the Standard pricing tier of Azure Security Center incurs an additional cost per node.

Default Value:

By default, Free pricing tier is selected.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/updatesubscriptionpricing

CIS Controls:

Version 7

8 Malware Defenses

Malware Defenses

2.2 Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable automatic provisioning of the monitoring agent to collect security data.

Rationale:

When `Automatic provisioning of monitoring agent` is turned on, Azure Security Center provisions the Microsoft Monitoring Agent on all existing supported Azure virtual machines and any new ones that are created. The Microsoft Monitoring Agent scans for various security-related configurations and events such as system updates, OS vulnerabilities, endpoint protection, and provides alerts.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on `Edit Settings` each subscription
4. Click on `Data Collection`
5. Ensure that `Automatic provisioning of monitoring agent` is set to `On`

Azure Command Line Interface 2.0
Ensure the output of the below command is `On`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/au
toProvisioningSettings?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.autoProvision'
```

Remediation:

Azure Console

1. Go to `Security Center`

2. Click on `Security Policy`
3. Click On "Edit Settings" for each subscription
4. Click on `Data Collection`
5. Set `Automatic provisioning of monitoring agent` to `On`
6. Click `Save`

Azure Command Line Interface 2.0

Use the below command to set `Automatic provisioning of monitoring agent` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/au
toProvisioningSettings/default?api-version=2017-08-01-preview -
d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below.

```
   {
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/autoProvi
sioningSettings/default",
  "name": "default",
  "type": "Microsoft.Security/autoProvisioningSettings",
  "properties": {
    "autoProvision": "On"
  }
}
```

Impact:

None

Default Value:

By default, `Automatic provisioning of monitoring agent` is set to `On`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-data-security
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list

6. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

2.3 Ensure ASC Default policy setting "Monitor System Updates" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable system updates recommendations for virtual machines.

Rationale:

When this setting is enabled, it retrieves a daily list of available security and critical updates from Windows Update or Windows Server Update Services. The retrieved list depends on the service that's configured for that virtual machine and recommends that the missing updates be applied. For Linux systems, the policy uses the distro-provided package management system to determine packages that have available updates. It also checks for security and critical updates from Azure Cloud Services virtual machines.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription
5. Expand `Compute And Apps`
6. Ensure that `System updates` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not set to `Disabled` or empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.systemUpdatesMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor system updates` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Monitor System updates` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-apply-system-updates
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

2.4 Ensure ASC Default policy setting "Monitor OS Vulnerabilities" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable Monitor OS vulnerability recommendations for virtual machines.

Rationale:

When this setting is enabled, it analyzes operating system configurations daily to determine issues that could make the virtual machine vulnerable to attack. The policy also recommends configuration changes to address these vulnerabilities.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Compute And Apps`
6. Ensure that `Security Configurations` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not `Disabled` or empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.systemConfigurationsMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`

2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor os Vulnerabilities` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

Azure Security Center monitors security configurations using a set of over 150 recommended rules for hardening the OS, including rules related to firewalls, auditing, password policies, and more. Ensuring policy settings are ON and taking remediation actions for the recommendations will provide the appropriate level of security controls.

Default Value:

By default, `Monitor OS Vulnerabilities` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-remediate-os-vulnerabilities
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://gallery.technet.microsoft.com/Azure-Security-Center-a789e335
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
7. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

2.5 Ensure ASC Default policy setting "Monitor Endpoint Protection" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable Endpoint protection recommendations for virtual machines.

Rationale:

When this setting is enabled, it recommends endpoint protection be provisioned for all Windows virtual machines to help identify and remove viruses, spyware, and other malicious software.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Compute And Apps`
6. Ensure that `Endpoint protection` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not `Disabled` or Empty.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.endpointProtectionMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`

2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor Endpoint Protection` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Endpoint protection` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-install-endpoint-protection
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

2.6 Ensure ASC Default policy setting "Monitor Disk Encryption" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable Disk encryption recommendations for virtual machines.

Rationale:

When this setting is enabled, it recommends enabling disk encryption in all virtual machines (Windows and Linux as well) to enhance data protection at rest.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Compute And Apps`
6. Ensure that `Disk Encryption` is not set to `Disabled`

Azure Command Line Interface 2.0
Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.diskEncryptionMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`

3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor Disk Encryption` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Disk encryption` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-apply-disk-encryption
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

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.

2.7 Ensure ASC Default policy setting "Monitor Network Security Groups" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable Network security group recommendations for virtual machines.

Rationale:

When this setting is enabled, it recommends that network security groups be configured to control inbound and outbound traffic to VMs that have public endpoints. Network security groups that are configured for a subnet are inherited by all virtual machine network interfaces unless otherwise specified. In addition to checking that a network security group has been configured, this policy assesses inbound security rules to identify rules that allow incoming traffic.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Network`
6. Ensure that `Network Security Groups` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.networkSecurityGroupsMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor Network Security Groups` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Network security groups` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-network-security-groups
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

2.8 Ensure ASC Default policy setting "Monitor Web Application Firewall" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable Web application firewall recommendations for virtual machines.

Rationale:

When this setting is enabled, it recommends that a web application firewall is provisioned on virtual machines when either of the following is true:

- Instance-level public IP (ILPIP) is used and the inbound security rules for the associated network security group are configured to allow access to port 80/443.
- Load-balanced IP is used and the associated load balancing and inbound network address translation (NAT) rules are configured to allow access to port 80/443.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Network`
6. Ensure that `Web Application Firewall` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.webApplicationFirewallMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor Web Application Firewall` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Monitor Web Application Firewall` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-instance-level-public-ip
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-arm
6. https://docs.microsoft.com/en-us/azure/security-center/security-center-add-web-application-firewall
7. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
8. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

2.9 Ensure ASC Default policy setting "Enable Next Generation Firewall(NGFW) Monitoring" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable next generation firewall recommendations for virtual machines.

Rationale:

When this setting is enabled, it extends network protections beyond network security groups, which are built into Azure. Security Center will search for deployments where a next generation firewall is recommended and enable a virtual appliance to be provisioned.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Network`
6. Ensure that `Next generation firewall` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.nextGenerationFirewallMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`

2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Enable Next Generation Firewall(NGFW) Monitoring` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Next generation firewall` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-add-next-generation-firewall
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

2.10 Ensure ASC Default policy setting "Monitor Vulnerability Assessment" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable vulnerability assessment recommendations for virtual machines.

Rationale:

When this setting is enabled, it recommends a vulnerability assessment solution be installed on the VM.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Compute and Apps`
6. Ensure that `Vulnerability Assessment` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.vulnerabilityAssesmentMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`

3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor Vulnerability Assessment` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Vulnerability Assessment` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-vulnerability-assessment-recommendations
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

2.11 Ensure ASC Default policy setting "Monitor Storage Blob Encryption" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable storage encryption recommendations.

Rationale:

When this setting is enabled, any new data in Azure Blobs and Files will be encrypted.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Data`
6. Ensure that `Storage Encryption` is not set to `Disabled`

Azure Command Line Interface 2.0
Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.storageEncryptionMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`

4. In section `PARAMETERS`, Set `Monitor Storage Blob Encryption` to `Audit` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `Storage Encryption` is set to `Audit`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-encryption-for-storage-account
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

13 Data Protection
Data Protection

2.12 Ensure ASC Default policy setting "Monitor JIT Network Access" is not "Disabled" (Scored)

Profile Applicability:

- Level 2

Description:

Enable JIT Network Access for virtual machines.

Rationale:

When this setting is enabled, Security Center locks down inbound traffic to the Azure VMs by creating an NSG rule. The user can select the ports on the VM where inbound traffic should be locked down. Just in time virtual machine (VM) access can be used to lock down inbound traffic to the Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Network`
6. Ensure that `JIT Network Access` is not set to `Disabled`

Azure Command Line Interface 2.0
Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.jitNetworkAccessMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor JIT Network Access` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

Enabling this recommendation involves cost implications as this feature is not available with `Free Pricing Tier`.

Default Value:

With `Standard` pricing tier, `JIT Network Access` is set to `AuditIfNotExists` by default.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

9.4 Apply Host-based Firewalls or Port Filtering

Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

2.13 Ensure ASC Default policy setting "Monitor Adaptive Application Whitelisting" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable adaptive application controls.

Rationale:

Adaptive application controls help control which applications can run on VMs located in Azure, which among other benefits helps harden those VMs against malware. The Security Center uses machine learning to analyze the processes running in the VM and helps to apply white-listing rules using this intelligence.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Compute and Apps`
6. Ensure that `Adaptive Application controls` is not set to `Disabled`

Azure Command Line Interface 2.0
Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.adaptiveApplicationControlsMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`

2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor Application Whitelisting` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

Enabling this recommendation involves cost implications as this feature is not available with `Free Pricing Tier`.

Default Value:

With `Standard` pricing tier, `Adaptive Application Controls` is set to `AuditIfNotExists` by default.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

2.7 Utilize Application Whitelisting

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

2.14 Ensure ASC Default policy setting "Monitor SQL Auditing" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable SQL auditing recommendations.

Rationale:

When this setting is enabled, it recommends that access auditing for the Azure Database be enabled for compliance, advanced threat detection, and for investigation purposes.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Data`
6. Ensure that `SQL Auditing` is not set to `Disabled`

Azure Command Line Interface 2.0
Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.sqlAuditingMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`

3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor SQL Auditing` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `SQL Auditing` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-auditing-on-sql-servers
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-auditing-on-sql-databases
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
7. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

2.15 Ensure ASC Default policy setting "Monitor SQL Encryption" is not "Disabled" (Scored)

Profile Applicability:

- Level 1

Description:

Enable SQL encryption recommendations.

Rationale:

When this setting is enabled, it recommends that encryption at rest be enabled for the Azure SQL Database, associated backups, and transaction log files. In the event of a data breach, it will not be readable.

Audit:

Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand `Data`
6. Ensure that `SQL Encryption` is not set to `Disabled`

Azure Command Line Interface 2.0

Ensure the output of the below command is not `Disabled` or Empty

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01' | jq
'select(.name=="SecurityCenterBuiltIn")'|jq
'.properties.parameters.sqlEncryptionMonitoringEffect.value'
```

Remediation:

Azure Console

1. Navigate to `Azure Policy`

2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, Set `Monitor SQL Encryption` to `AuditIfNotExists` or any other available value than `Disabled`
5. Click `Save`

Impact:

None

Default Value:

By default, `SQL Encryption` is set to `AuditIfNotExists`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-transparent-data-encryption
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create

CIS Controls:

Version 7

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.

2.16 Ensure that 'Security contact emails' is set (Scored)

Profile Applicability:

- Level 1

Description:

Provide a security contact email address.

Rationale:

Microsoft reaches out to the designated security contact in case its security team finds that the organization's resources are compromised. This ensures that the proper people are aware of any potential compromise in order to mitigate the risk in a timely fashion.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on `Edit Settings` for the security policy subscription
4. Click on `Email notifications`
5. Ensure that a valid security contact email address is set

Azure Command Line Interface 2.0
Ensure the output of the below command is set not empty and is set with appropriate email ids.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default1")'|jq '.properties.email'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click On `Edit Settings` for the security policy subscription
4. Click on `Email notifications`

5. Set a valid email address for the security contact
6. Click `Save`

Azure Command Line Interface 2.0

Use the below command to set `Security contact emails` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below. And replace validEmailAddress with email ids csv for multiple.

```
    {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
      "name": "default1",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "phone": "<phone_number>",
        "alertNotifications": "On",
        "alertsToAdmins": "On"
      }
    }
```

Impact:

None

Default Value:

By default, `Email notifications` is not set.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/update

CIS Controls:

Version 7

3 Continuous Vulnerability Management
Continuous Vulnerability Management

2.17 Ensure that security contact 'Phone number' is set (Scored)

Profile Applicability:

- Level 1

Description:

Provide a security contact phone number.

Rationale:

Microsoft reaches out to the designated security contact in case its security team finds that the organization's resources are compromised. This ensures that the proper people are aware of any potential compromise in order to mitigate the risk in a timely fashion.

Before taking any action, make sure that the information provided is valid, as the communication is not digitally signed.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click On `Edit Settings` for the security policy subscription
4. Click on `Email notifications`
5. Ensure that a valid security contact Phone number is set

Azure Command Line Interface 2.0
Ensure the output of the below command is set not empty, and is set with appropriate phone number.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default1")'|jq '.properties.phone'
```

Remediation:

Azure Console

1. Go to `Security Center`

2. Click on `Security Policy`
3. Click On `Edit Settings` for the security policy subscription
4. Click on `Email notifications`
5. Set a valid security contact Phone number
6. Click `Save`

Azure Command Line Interface 2.0

Use the below command to set `security contact 'Phone number'`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below.
And replace `validEmailAddress` with email ids csv for multiple and `phoneNumber` with valid phone number.

```
       {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
      "name": "default1",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "phone": "<phone_number>",
        "alertNotifications": "On",
        "alertsToAdmins": "On"
      }
    }
```

Impact:

None

Default Value:

By default, a security contact Phone number is not set.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/update

CIS Controls:

Version 7

3 Continuous Vulnerability Management
Continuous Vulnerability Management

2.18 Ensure that 'Send email notification for high severity alerts' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable emailing security alerts to the security contact.

Rationale:

Enabling security alert emails ensures that security alert emails are received from Microsoft. This ensures that the right people are aware of any potential security issues and are able to mitigate the risk.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click On "Edit Settings" for the security policy subscription
4. Click on `Email notifications`
5. Ensure that `Send email notification for high severity alerts` is set to `On`

Azure Command Line Interface 2.0
Ensure the output of below command is set to `true`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default1")'|jq '.properties.alertNotifications'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click On `Edit Settings` for the security policy subscription
4. Click on `Email notifications`

5. Set `Send email notification for high severity alerts` to `On`
6. Click `Save`

Azure Command Line Interface 2.0

Use the below command to set `Send email notification for high severity alerts` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below.
And replace `validEmailAddress` with email ids csv for multiple and `phoneNumber` with valid phone number.

```
       {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
      "name": "default1",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "phone": "<phone_number>",
        "alertNotifications": "On",
        "alertsToAdmins": "On"
      }
    }
```

Impact:

None

Default Value:

By default, `Send email notification for high severity alerts` is not set.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/update

CIS Controls:

Version 7

3 Continuous Vulnerability Management
Continuous Vulnerability Management

2.19 Ensure that 'Send email also to subscription owners' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable security alert emails to subscription owners.

Rationale:

Enabling security alert emails to subscription owners ensures that they receive security alert emails from Microsoft. This ensures that they are aware of any potential security issues and can mitigate the risk in a timely fashion.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click On `Edit Settings` for the security policy subscription
4. Click on `Email notifications`
5. Ensure that `Send email also to subscription owners` is set to `On`

Azure Command Line Interface 2.0
Ensure the output of below command is set to `true`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default1")'|jq '.properties.alertsToAdmins'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click On `Edit Settings` for the security policy subscription
4. Click on `Email notifications`

5. Set `Send email also to subscription owners` to `On`
6. Click `Save`

Azure Command Line Interface 2.0

Use the below command to set `Send email also to subscription owners` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below.
And replace `validEmailAddress` with email ids csv for multiple and `phoneNumber` with valid phone number.

```
    {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
      "name": "default1",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "phone": "<phone_number>",
        "alertNotifications": "On",
        "alertsToAdmins": "On"
      }
    }
```

Impact:

None

Default Value:

By default, `Send email also to subscription owners` is not set.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/update

CIS Controls:

Version 7

3 Continuous Vulnerability Management
Continuous Vulnerability Management

3 Storage Accounts

This section covers security recommendations to follow to set storage account policies on an Azure Subscription. An Azure storage account provides a unique namespace to store and access Azure Storage data objects.

3.1 Ensure that 'Secure transfer required' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Enable data encryption is transit.

Rationale:

The secure transfer option enhances the security of a storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access storage accounts, the connection must use HTTPS. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. Because Azure storage doesn't support HTTPS for custom domain names, this option is not applied when using a custom domain name.

Audit:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Configuration`
3. Ensure that `Secure transfer required` is set to `Enabled`

Azure Command Line Interface 2.0

Use the below command to ensure the `Secure transfer required` is enabled for all the `Storage Accounts` by ensuring the output contains `true` for each of the `Storage Accounts`.

```
az storage account list --query [*].[name,enableHttpsTrafficOnly]
```

Remediation:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Configuration`
3. Set `Secure transfer required` to `Enabled`

Azure Command Line Interface 2.0

Use the below command to enable `Secure transfer required` for a `Storage Account`

```
az storage account update --name <storageAccountName> --resource-group
<resourceGroupName> --https-only true
```

Impact:

None

Default Value:

By default, `Secure transfer required` is set to `Disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/storage/storage-security-guide#encryption-in-transit
2. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_list
3. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_update

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit

Encrypt all sensitive information in transit.

3.2 Ensure that storage account access keys are periodically regenerated (Not Scored)

Profile Applicability:

- Level 1

Description:

Regenerate storage account access keys periodically.

Rationale:

When a storage account is created, Azure generates two 512-bit storage access keys, which are used for authentication when the storage account is accessed. Rotating these keys periodically ensures that any inadvertent access or exposure does not result in these keys being compromised.

Audit:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Activity log`
3. Under `Timespan` drop-down, select `Custom` and choose `Start time` and `End time` such that it ranges 90 days
4. Enter `RegenerateKey` in the `Search` text box
5. Click `Apply`

It should list out all `RegenerateKey` events. If no such event exists, then this is a finding.
Azure Command Line Interface 2.0
Step 1 - Get a list of storage accounts

```
az storage account list
```

Make a note of `id`, `name` and `resourceGroup`.
Step 2
For every storage account make sure that key is regenerated in past 90 days.

```
az monitor activity-log list --resource-group
```

The output should contain

```
"authorization"/"scope": <your_storage_account> AND "authorization"/"action":
"Microsoft.Storage/storageAccounts/regenerateKey/action" AND
"status"/"localizedValue": "Succeeded" "status"/"Value": "Succeeded" AND
"eventTimestamp" : (Should return time and date should be less than past 90
days)
```

Remediation:

Follow Microsoft Azure documentation for regenerating storage account access keys.

Impact:

Regenerating access keys can affect services in Azure as well as the organization's applications that are dependent on the storage account. All clients that use the access key to access the storage account must be updated to use the new key.

Default Value:

By default, access keys are not regenerated periodically.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-create-storage-account#regenerate-storage-access-keys

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

3.3 Ensure Storage logging is enabled for Queue service for read, write, and delete requests (Not Scored)

Profile Applicability:

- Level 2

Description:

The Storage Queue service stores messages that may be read by any client who has access to the storage account. A queue can contain an unlimited number of messages, each of which can be up to 64KB in size using version 2011-08-18 or newer. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the queues. Storage Logging log entries contain the following information about individual requests: Timing information such as start time, end-to-end latency, and server latency, authentication details , concurrency information and the sizes of the request and response messages.

Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

Audit:

- Go to `Storage Accounts`.
- Select the specific Storage Account.
- Use the `Diagnostics logs (classic)` blade from `Monitoring (classic)` section.
- Ensure the `Status` is set to `On`, if set to `Off`.
- Select `Queue properties`.
- Ensure `Read` `Write` `Delete` options are selected under the `Logging` section.

Via CLI :
Ensure the below command's output contains properties `delete`, `read` and `write` set to `true`.

```
az storage logging show --services q --account-name <storageAccountName>
```

Remediation:

- Go to `Storage Accounts`.
- Select the specific Storage Account.
- Use the `Diagnostics logs (classic)` blade from `Monitoring (classic)` section.
- Set the `Status` to `On`, if set to `Off`.
- Select `Queue properties`.
- Select `Read`, `Write` and `Delete` options under the `Logging` section to enable Storage Logging for Queue service.

Via CLI :
Use the below command to enable the Storage Logging for Queue service.

```
az storage logging update --account-name <storageAccountName> --account-key
<storageAccountKey> --services q --log rwd --retention 90
```

References:

1. https://docs.microsoft.com/en-us/rest/api/storageservices/enabling-storage-logging-and-accessing-log-data
2. https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging
3. https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

3.4 Ensure that shared access signature tokens expire within an hour (Not Scored)

Profile Applicability:

- Level 1

Description:

Expire shared access signature tokens within an hour.

Rationale:

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. A shared access signature can be provided to clients who should not be trusted with the storage account key but for whom it may be necessary to delegate access to certain storage account resources. Providing a shared access signature URI to these clients allows them access to a resource for a specified period of time. This time should be set as low as possible, and preferably no longer than an hour.

Audit:

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

Remediation:

When generating shared access signature tokens, use start and end time such that it falls within an hour.

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature

CIS Controls:

Version 7

16.10 Ensure All Accounts Have An Expiration Date

Ensure that all accounts have an expiration date that is monitored and enforced.

3.5 Ensure that shared access signature tokens are allowed only over https (Not Scored)

Profile Applicability:

- Level 1

Description:

Shared access signature tokens should be allowed only over HTTPS protocol.

Rationale:

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. A shared access signature can be provided to clients who should not be trusted with the storage account key but for whom it may be necessary to delegate access to certain storage account resources. Providing a shared access signature URI to these clients allows them access to a resource for a specified period of time. It is recommended to allow such access requests over HTTPS protocol only.

Audit:

Currently, SAS token protocols cannot be audited. Until Microsoft makes SAS transfer protocols a setting rather than a token creation parameter, this recommendation will require a manual verification.

Remediation:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Shared access signature`
3. Set `Allowed protocols` to `HTTPS only`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Impact:

None

Default Value:

By default, shared access signature tokens are allowed only over https protocol.

References:

1. https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

3.6 Ensure that 'Public access level' is set to Private for blob containers (Scored)

Profile Applicability:

- Level 1

Description:

Disable anonymous access to blob containers.

Rationale:

Anonymous, public read access to a container and its blobs can be enabled in Azure Blob storage. It grants read-only access to these resources without sharing the account key, and without requiring a shared access signature. It is recommended not to provide anonymous access to blob containers until, and unless, it is strongly desired. A shared access signature token should be used for providing controlled and timed access to blob containers.

Audit:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Containers` under `BLOB SERVICE`
3. For each container, click `Access policy`
4. Ensure that `Public access level` is set to `Private (no anonymous access)`

Azure Command Line Interface 2.0
Ensure the below command output contains null

```
az storage container list  --account-name <accountName> --account-key
<accountKey> --query '[*].properties.publicAccess'
```

Remediation:

Azure Console
First, follow Microsoft documentation and created shared access signature tokens for your blob containers. Then,

1. Go to `Storage Accounts`
2. For each storage account, go to `Containers` under `BLOB SERVICE`
3. For each container, click `Access policy`
4. Set `Public access level` to `Private (no anonymous access)`

Azure Command Line Interface 2.0

1. Identify the container name from the audit command
2. Set the permission for public access to `private`(off) for the above container name, using the below command

```
az storage container set-permission --name <containerName> --public-access
off --account-name <accountName> --account-key <accountKey>
```

Impact:

Access using shared access signatures will have to be managed.

Default Value:

By default, `Public access level` is set to `Private (no anonymous access)` for blob containers.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/storage-manage-access-to-resources

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

3.7 Ensure default network access rule for Storage Accounts is set to deny (Scored)

Profile Applicability:

- Level 2

Description:

Restricting default network access helps to provide a new layer of security, since storage accounts accept connections from clients on any network. To limit access to selected networks, the default action must be changed.

Rationale:

Storage accounts should be configured to deny access to traffic from all networks (including internet traffic). Access can be granted to traffic from specific Azure Virtual networks, allowing a secure network boundary for specific applications to be built. Access can also be granted to public internet IP address ranges, to enable connections from specific internet or on-premises clients. When network rules are configured, only applications from allowed networks can access a storage account. When calling from an allowed network, applications continue to require proper authorization (a valid access key or SAS token) to access the storage account.

Audit:

Azure Console

1. Go to Storage Accounts
2. For each `storage account`, Click on the settings menu called `Firewalls` and `virtual networks`.
3. Ensure that Allow access from `All networks` is not selected.

Azure Command Line Interface 2.0

Ensure `defaultAction` is not set to `Allow`.

```
az storage account list --query '[*].networkRuleSet'
```

Remediation:

Azure Console

1. Go to `Storage Accounts`

2. For each storage account, Click on the `settings` menu called `Firewalls` and `virtual networks`.
3. Ensure that you have elected to allow access from `Selected networks`.
4. Add rules to `allow traffic` from `specific network`.
5. Click Save to apply your changes.

Azure Command Line Interface 2.0

Use the below command to update `default-action` to `Deny`.

```
az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --default-action Deny
```

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

3.8 Ensure 'Trusted Microsoft Services' is enabled for Storage Account access (Not Scored)

Profile Applicability:

- Level 2

Description:

Some Microsoft services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Microsoft services to bypass the network rules. These services will then use strong authentication to access the storage account. If the Allow trusted Microsoft services exception is enabled, the following services: Azure Backup, Azure Site Recovery, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure Networking, Azure Monitor and Azure SQL Data Warehouse (when registered in the subscription), are granted access to the storage account.

Rationale:

Turning on firewall rules for storage account will block access to incoming requests for data, including from other Azure services. This includes using the Portal, writing logs, etc. We can re-enable functionality. The customer can get access to services like Monitor, Networking, Hubs, and Event Grid by enabling `"Trusted Microsoft Services"` through exceptions. Also, Backup and Restore of Virtual Machines using unmanaged disks in storage accounts with network rules applied is supported via creating an exception.

Audit:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, Click on the settings menu called `Firewalls` and `virtual networks`.
3. Click on `Selected networks`.
4. Ensure that `Allow trusted Microsoft services to access this storage account` is checked in `Exceptions`.

Azure Command Line Interface 2.0

Ensure `bypass` contains `AzureServices`

```
az storage account list --query '[*].networkRuleSet'
```

Remediation:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, Click on the settings menu called `Firewalls` and `virtual networks`.
3. Ensure that you have elected to allow access from 'Selected networks'.
4. Enable check box for `Allow trusted Microsoft services to access this storage account`.
5. Click Save to apply your changes.

Azure Command Line Interface 2.0

Use the below command to update `trusted Microsoft services`.

```
az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --bypass AzureServices
```

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

CIS Controls:

Version 7

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.

4 Database Services

This section covers security recommendations to follow to set general database services policies on an Azure Subscription. Subsections will address specific database types.

4.1 Ensure that 'Auditing' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable auditing on SQL Servers.

Rationale:

The Azure platform allows a SQL server to be created as a service. Enabling auditing at the server level ensures that all existing and newly created databases on the SQL server instance are audited. Auditing policy applied on the SQL database does not override auditing policy and settings applied on the particular SQL server where the database is hosted.

Auditing tracks database events and writes them to an audit log in the Azure storage account. It also helps to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Ensure that `Auditing` is set to `On`

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerAuditing -ResourceGroupName <resource group name> -
ServerName <server name>
```

Ensure that `AuditState` is set to `Enabled`.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Set `Auditing` to `On`

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server, enable auditing.

```
Set-AzureRmSqlServerAuditingPolicy -ResourceGroupName <resource group name> -
ServerName <server name> -AuditType <audit type> -StorageAccountName <storage
account name>
```

Impact:

None

Default Value:

By default, `Auditing` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-auditing-on-sql-servers
2. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserverauditing?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverauditingpolicy?view=azurermps-5.2.0
4. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing

CIS Controls:

Version 7

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.2 Ensure that 'AuditActionGroups' in 'auditing' policy for a SQL server is set properly (Scored)

Profile Applicability:

- Level 1

Description:

Configure the 'AuditActionGroups' property to appropriate groups to capture all the critical activities on the SQL Server and all the SQL databases hosted on the SQL server.

Rationale:

To capture all critical activities done on SQL Servers and databases within sql servers, auditing should be configured to capture appropriate 'AuditActionGroups'. Property `AuditActionGroup` should contains at least `SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP, FAILED_DATABASE_AUTHENTICATION_GROUP, BATCH_COMPLETED_GROUP` to ensure comprehensive audit logging for SQL servers and SQL databases hosted on SQL Server.

Audit:

Azure Console
On Azure Console, There is no provision to check or change `AuditActionGroup` property.
Azure PowerShell
Get the list of all SQL Servers
`Get-AzureRmSqlServer`
For each Server
`Get-AzureRmSqlServerAuditing -ResourceGroupName <resource group name> -ServerName <server name>`
Ensure that `AuditActionGroup` contains all of
`SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP, FAILED_DATABASE_AUTHENTICATION_GROUP, BATCH_COMPLETED_GROUP.`

Remediation:

Azure Console
On Azure Console, There is no Provision to check or change `AuditActionGroup` property.
Azure PowerShell
To create Audit profile with prescribed 'AuditActionGroup':

```
Set-AzureRmSqlServerAuditingPolicy -ResourceGroupName "<resourceGroup>" -
ServerName "<serverName>" -StorageAccountName "storageAccountName" -
```

```
AuditActionGroup "SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP",
"FAILED_DATABASE_AUTHENTICATION_GROUP" -RetentionInDays <number >= 90>
```

Default Value:

When Auditing for a Sql Server is enabled using Azure Portal , AuditActionGroup property is by default set to {SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP, FAILED_DATABASE_AUTHENTICATION_GROUP, BATCH_COMPLETED_GROUP}.

References:

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-2017#database-level-audit-action-groups
2. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverauditingpolicy?view=azurermps-6.5.0

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4.3 Ensure that 'Auditing' Retention is 'greater than 90 days' (Scored)

Profile Applicability:

- Level 1

Description:

SQL Server Audit Retention should be configured to be greater than 90 days.

Rationale:

Audit Logs can be used to check for anomalies and give insight into suspected breaches or misuse of information and access.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Select `Storage Details`
5. Ensure `Retention (days)` setting `greater than 90 days`

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerAuditing -ResourceGroupName <resource group name> -
ServerName <server name>
```

Ensure that `RetentionInDays` is set to `more than or equal to 90`

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Select `Storage Details`

5. Set `Retention (days)` setting `greater than 90 days`
6. Select `OK`
7. Select `Save`

Azure PowerShell

For each Server, set retention policy for more than or equal to 90 days

```
set-AzureRmSqlServerAuditing -ResourceGroupName <resource group name> -
ServerName <server name> -RetentionInDays <Number of Days to retain the audit
logs, should be 90days minimum>
```

Impact:

None

Default Value:

By default, SQL Server audit storage is `disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing
2. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserverauditing?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverauditing?view=azurermps-5.2.0

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

4.4 Ensure that 'Advanced Data Security' on a SQL server is set to 'On' (Scored)

Profile Applicability:

- Level 2

Description:

Enable "Advanced Data Security" on critical SQL Servers.

Rationale:

SQL Server "Advanced Data Security" provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Users will receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns. SQL Server Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat. Additionally, SQL server Advanced Data Security includes functionality for discovering and classifying sensitive data.

Advanced Data Security is a paid feature. It is recommended to enable the feature at least on business-critical SQL Servers.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Advanced Data Security`
4. Ensure that `Advanced Data Security` is set to `On`

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name>
```

Ensure that `ThreatDetectionState` is set to `Enabled`.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Advanced Data Security`
4. Set `Advanced Data Security` to `On`

Azure PowerShell

Enable `Advanced Data Security` for a SQL Server:

```
Set-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name> -EmailAdmins $True
```

Note:

- Enabling 'Advanced Data Security' from the Azure portal enables `Threat Detection`
- Using Powershell command `Set-AzureRmSqlServerThreatDetectionPolicy` enables `Advanced Data Security` for a SQL server

Impact:

Enabling the `Advanced Data Security` feature can incur additional costs for each SQL server.

Default Value:

By default, `Advanced Data Security` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-advanced-threat-protection
2. https://docs.microsoft.com/cs-cz/powershell/module/azurerm.sql/get-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

4.5 Ensure that 'Threat Detection types' is set to 'All' (Scored)

Profile Applicability:

- Level 2

Description:

Enable all types of threat detection on SQL servers.

Rationale:

Enabling all threat detection types protects against SQL injection, database vulnerabilities, and any other anomalous activities.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Advanced Data Security`
4. At section Threat Detection Settings, Ensure that `Threat Detection Types` is set to `All`

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name>
```

Ensure that `ExcludedDetectionTypes` is set to `{}` i.e.. None.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Advanced Data Security`
4. At section Threat Detection Settings, Set `Threat Detection types` to `All`

Azure PowerShell

For each Server, set `ExcludedDetectionTypes` to None:

```
Set-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name> -ExcludedDetectionType "None"
```

Impact:

None

Default Value:

By default, `Threat Detection types` is not set.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-advanced-threat-protection
2. https://docs.microsoft.com/cs-cz/powershell/module/azurerm.sql/get-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0

CIS Controls:

Version 7

3.1 Run Automated Vulnerability Scanning Tools

Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

4.6 Ensure that 'Send alerts to' is set (Scored)

Profile Applicability:

- Level 2

Description:

Provide the email address where alerts will be sent when anomalous activities are detected on SQL servers.

Rationale:

Providing the email address to receive alerts ensures that any detection of anomalous activities is reported as soon as possible, making it more likely to mitigate any potential risk sooner.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Advanced Data Security`
4. At section Threat Detection Settings, Ensure that `Send alerts to` is set as appropriate.

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name>
```

Ensure that `NotificationRecipientsEmails` is set to the `recipient email id`.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each server instance

3. Click on `Advanced Threat Protection`
4. Set `Send alerts to` as appropriate

Azure PowerShell

For each Server, set `Send alerts to`

```
Set-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name> -NotificationRecipientsEmails  "<Recipient
Email ID>"
```

Impact:

None

Default Value:

By default, `Send alerts to` is not set.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-advanced-threat-protection
2. https://docs.microsoft.com/cs-cz/powershell/module/azurerm.sql/get-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0

CIS Controls:

Version 7

19 Incident Response and Management
Incident Response and Management

4.7 Ensure that 'Email service and co-administrators' is 'Enabled' (Scored)

Profile Applicability:

- Level 2

Description:

Enable service and co-administrators to receive security alerts from the SQL server.

Rationale:

Providing the email address to receive alerts ensures that any detection of anomalous activities is reported as soon as possible, making it more likely to mitigate any potential risk sooner.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Advanced Data Security`
4. At section Threat Detection Settings, Ensure that `Email service and co-administrators` is `Enabled`

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name>
```

Ensure that `EmailAdmins` is set to `True`.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each server instance

3. Click on `Advanced Data Security`
4. At section Threat Detection Settings, Enable `Email service and co-administrators`

Azure PowerShell

For each Server, `enable Email service and co-administrators`

```
Set-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name> -EmailAdmins $True
```

Impact:

None

Default Value:

By default, `Email service and co-administrators` is enabled.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-advanced-threat-protection
2. https://docs.microsoft.com/cs-cz/powershell/module/azurerm.sql/get-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0

CIS Controls:

Version 7

19 Incident Response and Management
Incident Response and Management

4.8 Ensure that Azure Active Directory Admin is configured (Scored)

Profile Applicability:

- Level 1

Description:

Use Azure Active Directory Authentication for authentication with SQL Database.

Rationale:

Azure Active Directory authentication is a mechanism to connect to Microsoft Azure SQL Database and SQL Data Warehouse using identities in Azure Active Directory (Azure AD). With Azure AD authentication, identities of database users and other Microsoft services can be managed in one central location. Central ID management provides a single place to manage database users and simplifies permission management.

- It provides an alternative to SQL Server authentication.
- Helps stop the proliferation of user identities across database servers.
- Allows password rotation in a single place.
- Customers can manage database permissions using external (AAD) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Azure Active Directory.
- Azure AD authentication uses contained database users to authenticate identities at the database level.
- Azure AD supports token-based authentication for applications connecting to SQL Database.
- Azure AD authentication supports ADFS (domain federation) or native user/password authentication for a local Azure Active Directory without domain synchronization.
- Azure AD supports connections from SQL Server Management Studio that use Active Directory Universal Authentication, which includes Multi-Factor Authentication (MFA). MFA includes strong authentication with a range of easy verification options — phone call, text message, smart cards with pin, or mobile app notification.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each SQL server, click on `Active Directory admin`
3. Ensure that an AD account has been populated for field `Active Directory admin`

Azure PowerShell

Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure Output shows `DisplayName` set to `AD account`.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each SQL server, click on `Active Directory admin`
3. Click on `Set admin`
4. Select an admin
5. Click `Save`

Azure PowerShell

For each Server, set AD Admin

```
Set-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name> -DisplayName "<Display name of AD
account to set as DB administrator>"
```

Impact:

None

Default Value:

Azure Active Directory Authentication for SQL Database/Server is not enabled by default

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure
2. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserveractivedirectoryadministrator?view=azurermps-5.2.0

4. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserveractivedirectoryadministrator?view=azurermps-5.2.0

CIS Controls:

Version 7

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.

4.9 Ensure that 'Data encryption' is set to 'On' on a SQL Database (Scored)

Profile Applicability:

- Level 1

Description:

Enable Transparent Data Encryption on every SQL server.

Rationale:

Azure SQL Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

Audit:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Transparent data encryption`
4. Ensure that `Data encryption` is set to `On`

Azure Command Line Interface 2.0
Ensure the output of the below command is `Enabled`

```
az sql db tde show --resource-group <resourceGroup> --server <dbServerName> -
-database <dbName> --query status
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Transparent data encryption`
4. Set `Data encryption` to `On`

Azure Command Line Interface 2.0
Use the below command to enable `Transparent data encryption` for SQL DB instance.

```
az sql db tde set --resource-group <resourceGroup> --server <dbServerName> --
database <dbName> --status Enabled
```

Impact:

None

Default Value:

By default, `Data encryption` is set to `On`.

References:

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-with-azure-sql-database

CIS Controls:

Version 7

14.8 Encrypt Sensitive Information at Rest

Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.

4.10 Ensure SQL server's TDE protector is encrypted with BYOK (Use your own key) (Scored)

Profile Applicability:

- Level 2

Description:

TDE with BYOK support provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties.

With TDE, data is encrypted at rest with a symmetric key (called the database encryption key) stored in the database or data warehouse distribution. To protect this data encryption key (DEK) in the past, only a certificate that the Azure SQL Service managed could be used. Now, with BYOK support for TDE, the DEK can be protected with an asymmetric key that is stored in the Key Vault. Key Vault is a highly available and scalable cloud-based key store which offers central key management, leverages FIPS 140-2 Level 2 validated hardware security modules (HSMs), and allows separation of management of keys and data, for additional security.

Based on business needs or criticality of data/databases hosted a SQL server, it is recommended that the TDE protector is encrypted by a key that is managed by the data owner (BYOK).

Rationale:

Bring Your Own Key (BYOK) support for Transparent Data Encryption (TDE) allows user control of TDE encryption keys and restricts who can access them and when. Azure Key Vault, Azure's cloud-based external key management system is the first key management service where TDE has integrated support for BYOK. With BYOK, the database encryption key is protected by an asymmetric key stored in the Key Vault. The asymmetric key is set at the server level and inherited by all databases under that server. This feature is currently in preview and we do not recommend using it for production workloads until we declare General Availability.

Audit:

Azure Portal:

1. Go to `SQL servers`

2. For the desired server instance
3. Click On `Transparent data encryption`
4. Ensure that `Use your own key` is set to `YES`
5. Ensure `Make selected key the default TDE protector` is checked

Azure CLI:

```
az account get-access-token --query
"{subscripton:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json" GET
https://management.azure.com/subscriptions/$0/resourceGroups/{resourceGroupNa
me}/providers/Microsoft.Sql/servers/{serverName}/encryptionProtector?api-
version=2015-05-01-preview'
```

Ensure the output of the command contains properties

`kind` set to `azurekeyvault`

`serverKeyType` set to `AzureKeyVault`

`uri` is not null

Remediation:

Azure Console:

Go to `SQL servers`

For the desired server instance

1. Click On `Transparent data encryption`
2. Set `Use your own key` to `YES`
3. Browse through your `key vaults` to Select an existing key or create a new key in Key Vault.
4. Check `Make selected key the default TDE protector`

Azure CLI:

Use the below command to encrypt SQL server's TDE protector with BYOK

```
az sql server tde-key >> Set --resource-group <resourceName> --server
<dbServerName> --server-key-type {AzureKeyVault} [--kid <keyIdentifier>]```
```

Impact:

Once TDE protector is encrypted with BYOK, it transfers entire responsibility of respective key management on you and hence you should be more careful about doing any operations on the particular key in order to keep data from corresponding SQL server and Databases hosted accessible.

Default Value:

By Default, Microsoft managed TDE protector is enabled for a SQL server. By default option 'Use your own key' is set to 'ON'.

References:

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-byok-azure-sql
2. https://azure.microsoft.com/en-in/blog/preview-sql-transparent-data-encryption-tde-with-bring-your-own-key-support/
3. https://winterdom.com/2017/09/07/azure-sql-tde-protector-keyvault

CIS Controls:

Version 7

16.4 Encrypt or Hash all Authentication Credentials
Encrypt or hash with a salt all authentication credentials when stored.

4.11 Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `SSL connection` on `MYSQL` Servers.

Rationale:

SSL connectivity helps to provide a new layer of security, by connecting database server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure- list text here.com
2. Go to `Azure Database` for `MySQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings
5. Ensure `Enforce SSL connection` is set to `ENABLED`.

Azure Command Line Interface 2.0
Ensure the output of the below command returns ENABLED.

```
az mysql server show --resource-group myresourcegroup --name
<resourceGroupName> --query sslEnforcement
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `MySQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings
5. Click on `ENABLED` for `Enforce SSL connection`

Azure Command Line Interface 2.0

Use the below command to set MYSQL Databases to Enforce SSL connection.

```
az mysql server update --resource-group <resourceGroupName> --name
<serverName> --ssl-enforcement Enabled
```

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit

Encrypt all sensitive information in transit.

4.12 Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `log_checkpoints` on `PostgreSQL Servers`.

Rationale:

Enabling `log_checkpoints` helps the PostgreSQL Database to `Log each checkpoint` in turn generates query and error logs. However, access to transaction logs is not supported. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to Azure `Database` for `PostgreSQL` server
3. For each database, click on `Server parameters`
4. Search for `log_checkpoints`.
5. Ensure that value is set to `ON`.

Azure Command Line Interface 2.0

Ensure value is set to `ON`

```
az postgres server configuration show  --resource-group <resourceGroupName> -
-server-name <serverName> --name log_checkpoints
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_checkpoints`.
5. Click `ON` and save.

Azure Command Line Interface 2.0

Use the below command to update `log_checkpoints` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name log_checkpoints --value on
```

References:

1. https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

4.13 Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `SSL connection` on `PostgreSQL` Servers.

Rationale:

`SSL connectivity` helps to provide a new layer of security, by connecting database server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database for PostgreSQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings
5. Ensure `Enforce SSL connection` is set to `ENABLED`.

Azure Command Line Interface 2.0
Ensure the output of the below command returns ENABLED.

```
az postgres server show --resource-group myresourcegroup --name
<resourceGroupName> --query sslEnforcement
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to Azure Database for `PostgreSQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings.
5. Click on `ENABLED` to Enforce SSL connection

Azure Command Line Interface 2.0

Use the below command to `enforce ssl connection` for `PostgreSQL` Database.

```
az postgres server update --resource-group <resourceGroupName> --name
<serverName> --ssl-enforcement Enabled
```

References:

1. https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal#prerequisites

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit

Encrypt all sensitive information in transit.

4.14 Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `log_connections` on `PostgreSQL Servers`.

Rationale:

Enabling `log_connections` helps PostgreSQL Database to log attempted connection to the server, as well as successful completion of client authentication. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_connections`.
5. Ensure that value is set to `ON`.

Azure Command Line Interface 2.0

Ensure `log_connections` value is set to `ON`

```
az postgres server configuration show --resource-group <resourceGroupName> --
server-name <serverName> --name log_connections
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_connections`.
5. Click `ON` and save.

Azure Command Line Interface 2.0

Use the below command to update `log_connections` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name log_connections --value on
```

Default Value:

By default `log_connections` is disabled (set to `off`).

References:

1. https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

4.15 Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `log_disconnections` on `PostgreSQL Servers`.

Rationale:

Enabling `log_disconnections` helps PostgreSQL Database to `Logs end of a session`, including duration, which in turn generates query and error logs. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_disconnections`.
5. Ensure that value is set to `ON`.

Azure Command Line Interface 2.0

Ensure `log_connections` value is set to `ON`

```
az postgres server configuration show --resource-group <resourceGroupName> --
server-name <serverName> --name log_disconnections
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_disconnections`.
5. Click `ON` and save.

Azure Command Line Interface 2.0

Use the below command to update `log_disconnections` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name log_disconnections --value on
```

References:

1. https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

4.16 Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `log_duration` on `PostgreSQL Servers`.

Rationale:

Enabling `log_duration` helps the PostgreSQL Database to `Logs the duration of each completed SQL statement` which in turn generates query and error logs. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_duration`.
5. Ensure that value is set to `ON`.

Azure Command Line Interface 2.0

Ensure `log_duration` value is set to `ON`

```
az postgres server configuration show --resource-group <resourceGroupName> --
server-name <serverName> --name log_duration
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_duration`.
5. Click `ON` and save.

Azure Command Line Interface 2.0

Use the below command to update `log_duration` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name log_duration --value on
```

References:

1. https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

4.17 Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `connection_throttling` on `PostgreSQL Servers`.

Rationale:

Enabling `connection_throttling` helps the PostgreSQL Database to `Set the verbosity of logged messages` which in turn generates query and error logs with respect to concurrent connections, that could lead to a successful Denial of Service (DoS) attack by exhausting connection resources. A system can also fail or be degraded by an overload of legitimate users. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `connection_throttling`.
5. Ensure that value is set to `ON`.

Azure Command Line Interface 2.0

Ensure `connection_throttling` value is set to `ON`

```
az postgres server configuration show --resource-group <resourceGroupName> --
server-name <serverName> --name connection_throttling
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `connection_throttling`.

5. Click ON and save.

Azure Command Line Interface 2.0

Use the below command to update `connection_throttling` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name connection_throttling --value on
```

References:

1. https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver

CIS Controls:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

4.18 Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Scored)

Profile Applicability:

- Level 1

Description:

Enable `log_retention_days` on `PostgreSQL Servers`.

Rationale:

Enabling `log_retention_days` helps PostgreSQL Database to `Sets number of days a log file is retained` which in turn generates query and error logs. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_retention_days`.
5. Ensure that `value greater than 3`.

Azure Command Line Interface 2.0

Ensure `log_retention_days` value is greater than 3.

```
az postgres server configuration show --resource-group <resourceGroupName> --
server-name <serverName> --name log_retention_days
```

Remediation:

Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_retention_days`.
5. Enter value in range 4-7 (inclusive) and save.

Azure Command Line Interface 2.0

Use the below command to update `log_retention_days` configuration.

```
 az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name log_retention_days --value <4-7>
```

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

4.19 Ensure that Azure Active Directory Admin is configured (Scored)

Profile Applicability:

- Level 1

Description:

Use Azure Active Directory Authentication for authentication with SQL Database.

Rationale:

Azure Active Directory authentication is a mechanism to connect to Microsoft Azure SQL Database and SQL Data Warehouse by using identities in Azure Active Directory (Azure AD). With Azure AD authentication, identities of database users and other Microsoft services can be managed in one central location. Central ID management provides a single place to manage database users and simplifies permission management.

- It provides an alternative to SQL Server authentication.
- Helps stop the proliferation of user identities across database servers.
- Allows password rotation in a single place.
- Customers can manage database permissions using external (AAD) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Azure Active Directory.
- Azure AD authentication uses contained database users to authenticate identities at the database level.
- Azure AD supports token-based authentication for applications connecting to SQL Database.
- Azure AD authentication supports ADFS (domain federation) or native user/password authentication for a local Azure Active Directory without domain synchronization.
- Azure AD supports connections from SQL Server Management Studio that use Active Directory Universal Authentication, which includes Multi-Factor Authentication (MFA). MFA includes strong authentication with a range of easy verification options: phone call, text message, smart cards with pin, or mobile app notification.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each SQL server, click on `Active Directory admin`
3. Ensure that an AD account has been populated for field `Active Directory admin`

Azure PowerShell

Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure Output shows `DisplayName` set to `AD account`.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each SQL server, click on `Active Directory admin`
3. Click on `Set admin`
4. Select an admin
5. Click `Save`

Azure PowerShell

For each Server, set AD Admin

```
Set-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name> -DisplayName "<Display name of AD
account to set as DB administrator>"
```

Impact:

None

Default Value:

Azure Active Directory Authentication for SQL Database/Server is not enabled by default

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure
2. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserveractivedirectoryadministrator?view=azurermps-5.2.0

4. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserveractivedirectoryadministrator?view=azurermps-5.2.0

CIS Controls:

Version 7

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.

5 Logging and Monitoring

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

5.1 Configuring Log Profile

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

5.1.1 Ensure that a Log Profile exists (Scored)

Profile Applicability:

- Level 1

Description:

Enable log profile for exporting activity logs.

Rationale:

A log profile controls how an activity log is exported. By default, activity logs are retained only for 90 days. Log profiles should be defined so that logs can be exported and stored for a longer duration in order to analyze security activities within an Azure subscription.

Audit:

Azure Console

1. Go to `Activity log`
2. Ensure that a Log Profile is set

Azure Command Line Interface 2.0
Use the below command to list the Log Profiles and ensure at least one Log Profile exists.

```
az monitor log-profiles list --query [*].[id,name]
```

Remediation:

Azure Console

1. Go to `Activity log`
2. Click on `Export`
3. Configure the setting
4. Click on `Save`

Azure Command Line Interface 2.0
Use the below command to create a Log Profile in Azure Monitoring.

```
az monitor log-profiles create --categories <space separated category values
Write|Delete| Action> --days <numberofDaysForRetention> --enabled true --
location <locationName> --locations <Space separated list of regions> --name
<logprofileName>
```

Impact:

None

Default Value:

By default, log profile is not set.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs#export-the-activity-log-with-a-log-profile
2. https://docs.microsoft.com/en-us/cli/azure/monitor/log-profiles?view=azure-cli-latest#az_monitor_log_profiles_create

CIS Controls:

Version 7

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

5.1.2 Ensure that Activity Log Retention is set 365 days or greater (Scored)

Profile Applicability:

- Level 1

Description:

Ensure activity log retention is set for 365 days or greater.

Rationale:

A log profile controls how the activity log is exported and retained. Since the average time to detect a breach is 210 days, the activity log should be retained for 365 days or more in order to have time to respond to any incidents.

Audit:

Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Ensure `Retention (days)` is set to `365` OR `Retention (days)` is set to `0`

Azure Command Line Interface 2.0
Ensure the below command output contains:
`days` set `365 or greater` and `enabled` set to `true`
OR
`days` set `0` and `enabled` set to `false`

```
az monitor log-profiles list --query [*].retentionPolicy
```

Note: Setting the `Retention (days)` to `0` from portal retains the data forever. Setting `Retention (days)` to 0 from portal sets `days` to `0` and `enabled` to `false`.

Remediation:

Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Set `Retention (days)` is set to `365` or `0`
4. Select `Save`

Azure Command Line Interface 2.0

Use the below command to set the `Activity log Retention (days)` to `365 or greater`.

```
az monitor log-profiles update --name <logProfileName> --set
retentionPolicy.days=<number of days> retentionPolicy.enabled=true
```

Use the below command to store logs for forever (indefinitely).

```
az monitor log-profiles update --name <logProfileName> --set
retentionPolicy.days=0 retentionPolicy.enabled=false
```

Note:

- If CLI command returns error by expecting location not set to null, append `location=global` in the command line. When log profile is set using azure portal, by default location is set to null and causes error when tried to update log profile using CLI.

Impact:

None

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-archive-activity-log

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Central Log Management

Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.

5.1.3 Ensure audit profile captures all the activities (Scored)

Profile Applicability:

- Level 1

Description:

The log profile should be configured to export all activities from the control/management plane.

Rationale:

A log profile controls how the activity log is exported. Configuring the log profile to collect logs for the categories "write", "delete" and "action" ensures that all the control/management plane activities performed on the subscription are exported.

Audit:

Azure Console
On the Azure Portal there is no provision to check or set categories. However, when a log profile is created using the Azure Portal, `Write, Delete and Action` categories are set by default.
Azure Command Line Interface 2.0
Ensure the categories set to `Write, Delete and Action`:

```
az monitor log-profiles list --query [*].categories
```

Remediation:

Azure Console
On Azure portal there is no provision to check or set categories.
Azure Command Line Interface 2.0
Use command: `az monitor log-profiles update --name default` in order to update existing default log profile.
Please refer to the documentation: `https://docs.microsoft.com/en-us/cli/azure/monitor/log-profiles?view=azure-cli-latest#az-monitor-log-profiles-update`

Default Value:

When the log profile is created using Azure Portal, by default it is configured to export categories - Write, Delete and Action. However, when the log profile is created using the command line, the user can explicitly choose which of the log categories to export.

References:

1. https://docs.microsoft.com/en-us/cli/azure/monitor/log-profiles?view=azure-cli-latest#az-monitor-log-profiles-update

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.1.4 Ensure the log profile captures activity logs for all regions including global (Scored)

Profile Applicability:

- Level 1

Description:

Configure the log profile to export activities from all Azure supported regions/locations including global.

Rationale:

A log profile controls how the activity Log is exported.

Ensuring that logs are exported from all the Azure supported regions/locations means that logs for potentially unexpected activities occurring in otherwise unused regions are stored and made available for incident response and investigations.

Including global region/location in the log profile locations ensures all events from the control/management plane will be exported, as many events in the activity log are global events.

Audit:

Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Select `Subscription`
4. Click `Regions` dropdown and ensure `Select all` is checked

Azure Command Line Interface 2.0

1. Count all azure supported regions:

```
az account list-locations --query [*].displayName | grep -P '\w+' | wc -l
```

2. Ensure the all azure supported regions are covered along with additional global region:

```
az monitor log-profiles list --query [*].locations | grep -P '\w+' | wc -l
```

This gives count which should be +1 (for global region) than count in command output 1

Remediation:

Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Select `Subscription`
4. In `Regions` dropdown list, check `Select all`
5. Select `Save`

Azure Command Line Interface 2.0

Use command: `az monitor log-profiles update --name default` in order to update existing default log profile.

Please refer to the documentation: `https://docs.microsoft.com/en-us/cli/azure/monitor/log-profiles?view=azure-cli-latest#az-monitor-log-profiles-update`

Default Value:

There is no default value.

References:

1. https://docs.microsoft.com/en-us/cli/azure/monitor/log-profiles?view=azure-cli-latest#az-monitor-log-profiles-update

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.1.5 Ensure the storage container storing the activity logs is not publicly accessible (Scored)

Profile Applicability:

- Level 1

Description:

The storage account container containing the activity log export should not be publicly accessible.

Rationale:

Allowing public access to activity log content may aid an adversary in identifying weaknesses in the affected account's use or configuration.

Audit:

Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Select `Subscription`https://workbench.cisecurity.org/sections/43928/recommendations/115705/edit#
4. In section `Storage Account`, note the name of the Storage account
5. Close the `Export Audit Logs` blade. Close the `Monitor - Activity Log` blade.
6. In right column, Click service `Storage Accounts` to access Storage account blade
7. Click on the storage account name noted in step 4. This will open blade specific to that storage account
8. In Section `Blob Service` click `Containers`. It will list all the containers in next blade
9. Look for a record with container named as `insight-operational-logs`. Click `. . .` from right most column to open `Context menu`
10. Click `Access Policy` from `Context Menu` and ensure `Public Access Level` is set to `Private (no anonymous access)`

Azure Command Line Interface 2.0

1. Get storage account id configured with log profile:

```
az monitor log-profiles list --query [*].storageAccountId
```

2. Ensure the container storing activity logs (insights-operational-logs) is not publicly accessible:

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

In command output ensure `publicAccess` is set to `null`

Remediation:

Azure Console

1. In right column, Click service `Storage Accounts` to access Storage account blade
2. Click on the storage account name
3. In Section `Blob Service` click `Containers`. It will list all the containers in next blade
4. Look for a record with container named as `insight-operational-logs`. Click . . . from right most column to open `Context menu`
5. Click `Access Policy` from `Context Menu` and set `Public Access Level` to `Private (no anonymous access)`

Azure Command Line Interface 2.0

```
az storage container set-permission --name insights-operational-logs --
account-name <Storage Account Name> --public-access off
```

Impact:

Configuring container `Access policy` to `private` will remove access from the container for everyone except owners of the storage account. Access policy needs to be set explicitly in order to allow access to other desired users.

Default Value:

By default, public access is set to null (allowing only private access) for a container with activity log export.

CIS Controls:

Version 7

6 Maintenance, Monitoring and Analysis of Audit Logs
Maintenance, Monitoring and Analysis of Audit Logs

5.1.6 Ensure the storage account containing the container with activity logs is encrypted with BYOK (Use Your Own Key) (Scored)

Profile Applicability:

- Level 2

Description:

The storage account with the activity log export container is configured to use BYOK (Use Your Own Key).

Rationale:

Configuring the storage account with the activity log export container to use BYOK (Use Your Own Key) provides additional confidentiality controls on log data as a given user must have read permission on the corresponding storage account and must be granted decrypt permission by the CMK.

Audit:

Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Select `Subscription`
4. In section `Storage Account`, note the name of the Storage account
5. Close the `Export Audit Logs` blade. Close the `Monitor - Activity Log` blade.
6. In right column, Click service `Storage Accounts` to access Storage account blade
7. Click on the storage account name noted in step 4. This will open blade specific to that storage account
8. In Section `SETTINGS` click `Encryption`. It will show `Storage service encryption` configuration pane.
9. Ensure `Use your own key` is checked and `Key URI` is set.

Azure Command Line Interface 2.0

1. Get storage account id configured with log profile:

```
az monitor log-profiles list --query [*].storageAccountId
```

2. Ensure the storage account is encrypted with CMK:

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

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

Remediation:

Azure Console

1. In right column, Click service `Storage Accounts` to access Storage account blade
2. Click on the storage account name
3. In Section `SETTINGS` click `Encryption`. It will show `Storage service encryption` configuration pane.
4. Check `Use your own key` which will expand `Encryption Key` Settings
5. Use option `Enter key URI` or `Select from Key Vault` to set up encryption with your own key

Azure Command Line Interface 2.0

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

Default Value:

By default, for a storage account `keySource` is set to `Microsoft.Storage` allowing encryption with vendor Managed key and not the BYOK (Use Your Own Key).

CIS Controls:

Version 7

6 Maintenance, Monitoring and Analysis of Audit Logs
Maintenance, Monitoring and Analysis of Audit Logs

5.1.7 Ensure that logging for Azure KeyVault is 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Monitoring how and when key vaults are accessed, and by whom enables an audit trail of interactions with confidential information, keys and certificates managed by Azure Keyvault. Enabling logging for Key Vault saves information in an Azure storage account that the user provides. This creates a new container named insights-logs-auditevent automatically for the specified storage account, and this same storage account can be used for collecting logs for multiple key vaults.

Audit:

Azure Console

1. Go to `Key vaults`
2. For each Key vault
3. Go to `Diagnostic Logs`
4. Click on `Edit Settings`
5. Ensure that `Archive to a storage account` is `Enabled`
6. Ensure that `AuditEvent` is checked and the retention days is set to `180 days or as appropriate`

Azure Command Line Interface 2.0
List all key vaults

```
az keyvault list
```

For each keyvault `id`

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

Ensure that `storageAccountId` is set as appropriate. Also, ensure that `category` and `days` are set. One of the sample outputs is as below.

```
"logs": [
        {
          "category": "AuditEvent",
          "enabled": true,
          "retentionPolicy": {
            "days": 180,
            "enabled": true
          }
        }
      ]
```

Remediation:

Follow Microsoft Azure documentation and setup Azure Key Vault Logging.

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-logging

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2 Monitoring using Activity Log Alerts

This section covers security recommendations to follow in order to set alerting and monitoring for critical activities on an Azure subscription.

5.2.1 Ensure that Activity Log Alert exists for Create Policy Assignment (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create Policy Assignment event.

Rationale:

Monitoring for create policy assignment events gives insight into changes done in "azure policy - assignments" and may reduce the time it takes to detect unsolicited changes.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/policyAssignments/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create policy assignment (policyAssignments)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.authorization/policyassignments/write"),enabled:.properti
es.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.authorization/policyassignments/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Create policy assignment`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Authorization/policyAssignments/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
```

```
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.2 Ensure that Activity Log Alert exists for Create or Update Network Security Group (Scored)

Profile Applicability:

- Level 1

Description:

Create an Activity Log Alert for the "Create" or "Update Network Security Group" event.

Rationale:

Monitoring for "Create" or "Update Network Security Group" events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create or Update Network Security Group (networkSecurityGroups)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/write"),enabled:.properties
.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`

- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Create or Update Network Security Groups`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Network/networkSecurityGroups/write",
        "field": "operationName"
      }
    ]
```

```
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

}

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.3 Ensure that Activity Log Alert exists for Delete Network Security Group (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Network Security Group event.

Rationale:

Monitoring for "Delete Network Security Group" events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/delete`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Delete Network Security Group (networkSecurityGroups)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/delete"),enabled:.propertie
s.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/delete",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Delete Network Security Groups`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Network/networkSecurityGroups/delete",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
```

```
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.4 Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update Network Security Group Rule event.

Rationale:

Monitoring for Create or Update Network Security Group Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/securityRules/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create or Update Security Rule (networkSecurityGroups/securityRules)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/securityrules/write"),enabl
ed:.properties.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`

- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/securityrules/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Create or Update Network Security Groups rule`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals":
"Microsoft.Network/networkSecurityGroups/securityRules/write",
        "field": "operationName"
      }
```

```
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.5 Ensure that activity log alert exists for the Delete Network Security Group Rule (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Network Security Group Rule event.

Rationale:

Monitoring for Delete Network Security Group Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Delete Security Rule (networkSecurityGroups/securityRules)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/securityrules/delete"),enab
led:.properties.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`

- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/securityrules/delete",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Delete Network Security Groups rule`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals":
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "field": "operationName"
      }
```

```
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.6 Ensure that Activity Log Alert exists for Create or Update Security Solution (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update Security Solution event.

Rationale:

Monitoring for Create or Update Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/securitySolutions/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create or Update Security Solutions (securitySolutions)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.security/securitysolutions/write"),enabled:.properties.en
abled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.security/securitysolutions/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Create or Update Security Solutions`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Security/securitySolutions/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
```

```
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.7 Ensure that Activity Log Alert exists for Delete Security Solution (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Security Solution event.

Rationale:

Monitoring for Delete Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/securitySolutions/delete`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Delete Security Solutions (securitySolutions)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.security/securitysolutions/delete"),enabled:.properties.e
nabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.security/securitysolutions/delete",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Delete Security Solutions`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Security/securitySolutions/delete",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
```

```
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.8 Ensure that Activity Log Alert exists for Create or Update or Delete SQL Server Firewall Rule (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update or Delete SQL Server Firewall Rule event.

Rationale:

Monitoring for Create or Update or Delete SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Sql/servers/firewallRules/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create/Update server firewall rule (servers/firewallRules)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.sql/servers/firewallrules/write"),enabled:.properties.ena
bled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`

- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.sql/servers/firewallrules/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Create or Update or Delete SQL Firewall Rule`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Sql/servers/firewallRules/write",
        "field": "operationName"
      }
```

```
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

5.2.9 Ensure that Activity Log Alert exists for Update Security Policy (Scored)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Update Security Policy event.

Rationale:

Monitoring for Update Security Policy events gives insight into changes to security policy and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/policies/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Update security policy (policies)" has "any" level with "any" status and event is initiated by "any"`

Azure Command Line Interface 2.0

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/microsoft.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.security/policies/write"),enabled:.properties.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.security/policies/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Update or Delete SQL Firewall Rule`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

Where `input.json` contains the Request body JSON data as mentioned below.

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Security/policies/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
```

```
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid

CIS Controls:

Version 7

6.3 Enable Detailed Logging

Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

6 Networking

This section covers security recommendations to follow in order to set networking policies on an Azure subscription.

6.1 Ensure that RDP access is restricted from the internet (Scored)

Profile Applicability:

- Level 1

Description:

Disable RDP access on network security groups from the Internet.

Rationale:

The potential security problem with using RDP over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on an Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Azure Console

1. For each VM, open the `Networking` blade
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for RDP such as
    - port = `3389`,
    - protocol = `TCP`,
    - Source = `Any` OR `Internet`

Azure Command Line Interface 2.0
List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "3389" or "*" or "[port range containing 3389]"
"direction" : "Inbound"
"protocol" : "TCP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Disable direct RDP access to your Azure Virtual Machines from the Internet. After direct RDP access from the Internet is disabled, you have other options you can use to access these virtual machines for remote management:

- Point-to-site VPN
- Site-to-site VPN
- ExpressRoute

Impact:

None

Default Value:

By default, RDP access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines

CIS Controls:

Version 7

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.

6.2 Ensure that SSH access is restricted from the internet (Scored)

Profile Applicability:

- Level 1

Description:

Disable SSH access on network security groups from the Internet.

Rationale:

The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Azure Console

1. Open the `Networking` blade for the specific Virtual machine in Azure portal
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for SSH such as
    - port = `22`,
    - protocol = `TCP`,
    - Source = `Any` OR `Internet`

Azure Command Line Interface 2.0
List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "22" or "*" or "[port range containing 22]"
"direction" : "Inbound"
"protocol" : "TCP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Disable direct SSH access to your Azure Virtual Machines from the Internet. After direct SSH access from the Internet is disabled, you have other options you can use to access these virtual machines for remote management:

- Point-to-site VPN
- Site-to-site VPN
- ExpressRoute

Impact:

None

Default Value:

By default, SSH access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines

CIS Controls:

Version 7

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.

6.3 Ensure no SQL Databases allow ingress 0.0.0.0/0 (ANY IP) (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that no SQL Databases allow ingress from 0.0.0.0/0 (ANY IP).

Rationale:

SQL Server includes a firewall to block access to unauthorized connections. More granular IP addresses can be defined by referencing the range of addresses available from specific datacenters.

By default, for a SQL server, a Firewall exists with StartIp of 0.0.0.0 and EndIP of 0.0.0.0 allowing access to all the Azure services.

Additionally, a custom rule can be set up with StartIp of 0.0.0.0 and EndIP of 255.255.255.255 allowing access from ANY IP over the Internet.

In order to reduce the potential attack surface for a SQL server, firewall rules should be defined with more granular IP addresses by referencing the range of addresses available from specific datacenters.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall / Virtual Networks`
4. Ensure that `Allow access to Azure services` to set to `OFF`
5. Ensure that no firewall rule exists with

- Start IP of `0.0.0.0`
- or other combinations which allows access to wider public IP ranges

Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerFirewallRule -ResourceGroupName <resource group name> -
ServerName <server name>
```

Ensure that `StartIpAddress` is not set to `0.0.0.0` or other combinations which allows access to wider public IP ranges including Windows Azure IP ranges.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall / Virtual Networks`
4. Set `Allow access to Azure services` to `OFF'
5. Set firewall rules to limit access to only authorized connections

Azure PowerShell

Disable Default Firewall Rule `Allow access to Azure services` :

```
Remove-AzureRmSqlServerFirewallRule -FirewallRuleName
"AllowAllWindowsAzureIps" -ResourceGroupName <resource group name> -
ServerName <server name>
```

Remove custom Firewall rule:

```
Remove-AzureRmSqlServerFirewallRule -FirewallRuleName "<firewallRuleName>" -
ResourceGroupName <resource group name> -ServerName <server name>
```

Set the appropriate firewall rules:

```
Set-AzureRmSqlServerFirewallRule -ResourceGroupName <resource group name> -
ServerName <server name> -FirewallRuleName "<Fw rule Name>" -StartIpAddress
"<IP Address other than 0.0.0.0>" -EndIpAddress "<IP Address other than
0.0.0.0 or 255.255.255.255>"
```

Impact:

Impact: Disabling `Allow access to Azure Services` will break all connections to SQL server and Hosted Databases unless custom IP specific rules are not added in Firewall Policy.

Default Value:

By default, setting `Allow access to Azure Services` is set to `ON` allowing access to all Windows Azure IP ranges.

References:

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-windows-firewall-for-database-engine-access?view=sql-server-2017
2. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserverfirewallrule?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverfirewallrule?view=azurermps-5.2.0
4. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/remove-azurermsqlserverfirewallrule?view=azurermps-5.2.0
5. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure
6. https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-set-database-firewall-rule-azure-sql-database?view=azuresqldb-current

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

6.4 Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Scored)

Profile Applicability:

- Level 2

Description:

Network Security Group Flow Logs should be enabled and the retention period is set to greater than or equal to 90 days.

Rationale:

Flow logs enable capturing information about IP traffic flowing in and out of network security groups. Logs can be used to check for anomalies and give insight into suspected breaches.

Audit:

Azure Console

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the Logs section
3. Select each Network Security Group from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting `greater than 90 days`

Azure Command Line Interface 2.0

```
az network watcher flow-log show --resource-group <resourceGroup> --nsg
<NameorID of the NetworkSecurityGroup> --query 'retentionPolicy'
```

Ensure that `enabled` is set to `true` and `days` is set to `greater then or equal to 90`.

Remediation:

Azure Console

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the Logs section
3. Select each Network Security Group from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting `greater than 90 days`
6. Select your storage account in the `Storage account` field

7. Select `Save`

Azure Command Line Interface 2.0

Enable the `NSG flow logs` and set the Retention (days) to greater than or equal to 90 days.

```
az network watcher flow-log configure --nsg <NameorID of the Network Security
Group> --enabled true --resource-group <resourceGroupName> --retention 91 --
storage-account <NameorID of the storage account to save flow logs>
```

Impact:

None

Default Value:

By default, Network Security Group Flow Logs are `disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview
2. https://docs.microsoft.com/en-us/cli/azure/network/watcher/flow-log?view=azure-cli-latest

CIS Controls:

Version 7

6.4 Ensure adequate storage for logs

Ensure that all systems that store logs have adequate storage space for the logs generated.

6.5 Ensure that Network Watcher is 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Enable Network Watcher for Azure subscriptions.

Rationale:

Network diagnostic and visualization tools available with Network Watcher help users understand, diagnose, and gain insights to the network in Azure.

Audit:

Azure Console

1. Go to `Network Watcher`
2. Ensure that the `STATUS` is set to `Enabled`

Azure Command Line Interface 2.0

```
az network watcher list
```

Ensure that for all regions, `provisioningState` is set to `Succeeded`.

Remediation:

Azure Console

1. Go to `Network Watcher`
2. Right click on the subscription name and click on `Enable network watcher in all regions`

Azure Command Line Interface 2.0

Configure the `Network Watcher` for your subscription

```
az network watcher configure --locations <locations space separated list> --
enabled [true] --resource-group <resourceGroupName> --tags key[=value]
key[=value]
```

Impact:

None

Default Value:

By default, Network Watcher is `disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
2. https://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az_network_watcher_list
3. https://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az_network_watcher_configure

CIS Controls:

Version 7

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.

12.1 Maintain an Inventory of Network Boundaries

Maintain an up-to-date inventory of all of the organization's network boundaries.

7 Virtual Machines

This section covers security recommendations to follow in order to set virtual machine policies on an Azure subscription.

7.1 Ensure that 'OS disk' are encrypted (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that OS disks (boot volumes) are encrypted, where possible.

Rationale:

Encrypting the IaaS VM's OS disk (boot volume) ensures that its entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads.

Audit:

Azure Console

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Disks`
4. Ensure that the `OS disk` has encryption set to `Enabled`

Azure Command Line Interface 2.0
Ensure the below command output is shown as `Encrypted`

```
az vm encryption show --name <VMName> --resource-group <resourceGroupName> --
query osDisk
```

Remediation:

Azure Console
Follow Microsoft Azure documentation.
Azure Command Line Interface 2.0
Use the below command to enable encryption for OS Disk for the specific VM.

```
az vm encryption enable --name <VMName> --resource-group <resourceGroupName>
--volume-type OS --aad-client-id <Client ID of AAD app> --aad-client-secret
<Client Secret of AAD app> --disk-encryption-keyvault
https://<vaultEndpoint>/secrets/<secretName>/<secretVersion>
```

Impact:

Encryption is available only on Standard tier VMs. This might cost you more.

Default Value:

By default, OS disks are not encrypted.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json

CIS Controls:

Version 7

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.

7.2 Ensure that 'Data disks' are encrypted (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that data disks (non-boot volumes) are encrypted, where possible.

Rationale:

Encrypting the IaaS VM's Data disks (non-boot volume) ensures that its entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads.

Audit:

Azure Console

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Disks`
4. Ensure that each disk under `Data disks` has encryption set to `Enabled`

Azure Command Line Interface 2.0
Ensure the below command output is shown as `Encrypted`

```
az vm encryption show --name <VMName> --resource-group <resourceGroupName> --
query dataDisk
```

Remediation:

Azure Console
Follow Microsoft Azure documentation.
Azure Command Line Interface 2.0
Use the below command to enable encryption for Data Disk for the specific VM.

```
az vm encryption enable --name <VMName> --resource-group <resourceGroupName>
--volume-type DATA --aad-client-id <Client ID of AAD app> --aad-client-secret
<Client Secret of AAD app> --disk-encryption-keyvault
https://<vaultEndpoint>/secrets/<secretName>/<secretVersion>
```

Impact:

Encryption is available only on Standard tier VMs. This might cost more.

Default Value:

By default, data disks are not encrypted.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json

CIS Controls:

Version 7

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.

7.3 Ensure that 'Unattached disks' are encrypted (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that unattached disks in a subscription are encrypted.

Rationale:

Encrypting the IaaS VM's 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.

Audit:

Azure Console
At the time of writing this recommendation, we haven't found any `encryption` setting for a disk in `Disks` blade.
Azure Command Line Interface 2.0
Ensure command below does not retruns any output.

```
az disk list --query '[? managedBy == `null`].{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/rest/api/compute/disks/update#encryptionsettings
-https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-update
```

Impact:

Encryption is available only on Standard tier VMs. This might cost you more.

Default Value:

By default, data disks are not encrypted.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption
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

CIS Controls:

Version 7

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.

7.4 Ensure that only approved extensions are installed (Not Scored)

Profile Applicability:

- Level 1

Description:

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.

Audit:

Azure Console

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Extensions`
4. Ensure that the listed extensions are approved for use.

Azure Command Line Interface 2.0
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
```

Remediation:

Azure Console

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Extensions`
4. If there are unapproved extensions, uninstall them.

Azure Command Line Interface 2.0

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>
```

Impact:

None

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

CIS Controls:

Version 7

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.

7.5 Ensure that the latest OS Patches for all Virtual Machines are applied (Not Scored)

Profile Applicability:

- Level 1

Description:

Ensure that the latest OS patches for all virtual machines are applied.

Rationale:

Windows and Linux virtual machines should be kept updated to:

- Address a specific bug or flaw
- Improve an OS or application's general stability
- Fix a security vulnerability

The Azure Security Center retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on which service is configured on a Windows VM. The security center also checks for the latest updates in Linux systems. If a VM is missing a system update, the security center will recommend system updates be applied.

Audit:

Azure Console

1. Go to `Security Center - Recommendations`
2. Ensure that there are no recommendations for `Apply system updates`

Alternatively, you can employ your own patch assessment and management tool to periodically assess, report and install the required security patches for your OS.
Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

Follow Microsoft Azure documentation to apply security patches from the security center. Alternatively, you can employ your own patch assessment and management tool to periodically assess, report and install the required security patches for your OS.

Impact:

None

Default Value:

By default, patches are not automatically deployed.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-apply-system-updates
2. https://docs.microsoft.com/en-us/azure/security/azure-security-iaas#manage-operating-systems

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools

Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

7.6 Ensure that the endpoint protection for all Virtual Machines is installed (Not Scored)

Profile Applicability:

- Level 1

Description:

Install endpoint protection for all virtual machines.

Rationale:

Installing endpoint protection systems (like Antimalware for Azure) provides for real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on Azure systems.

Audit:

Azure Console

1. Go to `Security Center - Recommendations`
2. Ensure that there are no recommendations for `Endpoint Protection not installed on Azure VMs`

Azure Command Line Interface 2.0

```
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.

Impact:

This brings an additional cost to you.

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

CIS Controls:

Version 7

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.

8 Other Security Considerations

This section covers security recommendations to follow in order to set general security and operational controls on an Azure Subscription.

8.1 Ensure that the expiration date is set on all keys (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that all keys in Azure Key Vault have an expiration time set.

Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration time) attribute identifies the expiration time on or after which the key MUST NOT be used for a cryptographic operation. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration time for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes.

Audit:

Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Then ensure that each key in the vault has `EXPIRATION DATE` set as appropriate

Azure Command Line Interface 2.0
Ensure that the output of the below command contains Key ID (kid), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault key list --vault-name <KEYVALUTNAME> --query
[*].[{"kid":kid},{"enabled":attributes.enabled},{"expires":attributes.expires
}]
```

Remediation:

Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to Yes
4. Set an appropriate `EXPIRATION DATE` on all keys.

Azure Command Line Interface 2.0

Update the `EXPIRATION DATE` for the key using below command.

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --
expires Y-m-d'T'H:M:S'Z'
```

Impact:

Keys cannot be used beyond their assigned expiration times respectively. Keys need to be rotated periodically wherever they are used.

Default Value:

By default, keys do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-keys

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

8.2 Ensure that the expiration date is set on all Secrets (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that all Secrets in the Azure Key Vault have an expiration time set.

Rationale:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The `exp` (expiration time) attribute identifies the expiration time on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration time for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Audit:

Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Secrets`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Ensure that each secret in the vault has `EXPIRATION DATE` set as appropriate

Azure Command Line Interface 2.0
Ensure that the output of the below command contains ID (id), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault secret list --vault-name <KEYVAULTNAME> --query
[*].[{"id":id},{"enabled":attributes.enabled},{"expires":attributes.expires}]
```

Remediation:

Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Secrets`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Set an appropriate `EXPIRATION DATE` on all secrets.

Azure Command Line Interface 2.0

Use the below command to set `EXPIRATION DATE` on the all secrets.

```
az keyvault secret set-attributes --name <secretName> --vault-name
<vaultName> --expires Y-m-d'T'H:M:S'Z'
```

Impact:

Secrets cannot be used beyond their assigned expiry times respectively. Secrets need to be rotated periodically wherever they are used.

Default Value:

By default, secrets do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-secrets

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

8.3 Ensure that Resource Locks are set for mission critical Azure resources (Not Scored)

Profile Applicability:

- Level 2

Description:

Resource Manager Locks provide a way for administrators to lock down Azure resources to prevent deletion of, or modifications to, a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and, when applied, will place restrictions on the resource for all users. These are very useful when there is have an important resource in a subscription that users should not be able to delete or change and can help prevent accidental and malicious changes or deletion.

Rationale:

As an administrator, it may be necessary to lock a subscription, resource group, or resource to prevent other users in the organization from accidentally deleting or modifying critical resources. The lock level can be set to to `CanNotDelete` or `ReadOnly` to achieve this purpose.

- `CanNotDelete` means authorized users can still read and modify a resource, but they can't delete the resource.
- `ReadOnly` means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Audit:

Azure Console

1. Navigate to the specific Azure Resource or Resource Group
2. Click on `Locks`
3. Ensure the lock is defined with name and description, type as `CanNotDelete` or `ReadOnly` as appropriate.

Azure Command Line Interface 2.0
Review the list of all locks set currently:

```
az lock list --resource-group <resourcegroupname> --resource-name
<resourcename> --namespace <Namespace> --resource-type <type> --parent ""
```

Remediation:

Azure Console

1. Navigate to the specific Azure Resource or Resource Group
2. For each of the mission critical resource, click on `Locks`
3. Click `Add`
4. Give the lock a name and a description, then select the type, `CanNotDelete` or `ReadOnly` as appropriate

Azure Command Line Interface 2.0
To lock a resource, provide the name of the resource, its resource type, and its resource group name.

```
az lock create --name <LockName> --lock-type <CanNotDelete/Read-only> --
resource-group <resourceGroupName> --resource-name <resourceName> --resource-
type <resourceType>
```

Default Value:

By default, no locks are set.

References:

1. https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources
2. https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-subscription-governance#azure-resource-locks

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

8.4 Ensure the key vault is recoverable (Scored)

Profile Applicability:

- Level 1

Description:

The key vault contains object keys, secrets and certificates. Accidental unavailability of a key vault can cause immediate data loss or loss of security functions (authentication, validation, verification, non-repudiation, etc.) supported by the key vault objects.

It is recommended the key vault be made recoverable by enabling the "Do Not Purge" and "Soft Delete" functions. This is in order to prevent loss of encrypted data including storage accounts, SQL databases, and/or dependent services provided by key vault objects (Keys, Secrets, Certificates) etc., as may happen in the case of accidental deletion by a user or from disruptive activity by a malicious user.

Rationale:

There could be scenarios where users accidently run delete/purge commands on key vault or attacker/malicious user does it deliberately to cause disruption. Deleting or purging a key vault leads to immediate data loss as keys encrypting data and secrets/certificates allowing access/services will become non-accessible. There are 2 key vault properties that plays role in permanent unavailability of a key vault.

1> `enableSoftDelete`:

Setting this parameter to true for a key vault ensures that even if key vault is deleted, Key vault itself or its objects remain recoverable for next 90days. In this span of 90 days either key vault/objects can be recovered or purged (permanent deletion). If no action is taken, after 90 days key vault and its objects will be purged.

2> `enablePurgeProtection`:

enableSoftDelete only ensures that key vault is not deleted permanently and will be recoverable for 90 days from date of deletion. However, there are chances that the key vault and/or its objects are accidentally purged and hence will not be recoverable. Setting enablePurgeProtection to "true" ensures that the key vault and its objects cannot be purged.

Enabling both the parameters on key vaults ensures that key vaults and their objects cannot be deleted/purged permanently.

Audit:

Via Azure Portal
Azure Portal does not have provision to update the respective configurations
Via Azure CLI 2.0
1> List all Resources of type Key Vaults:

```
az resource list --query "[?type=='Microsoft.KeyVault/vaults']"
```

2> For Every Key Vault ID ensure check parameters `enableSoftDelete` and `enablePurgeProtection` are set to enabled.

```
az resource show --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName>
```

Remediation:

To enable "Do Not Purge" and "Soft Delete" for a Key Vault:
Via Azure Portal
Azure Portal does not have provision to update the respective configurations
Via Azure CLI 2.0

```
az resource update --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName> --set properties.enablePurgeProtection=true
properties.enableSoftDelete=true
```

Impact:

Once purge-protection and soft-delete is enabled for a key vault, the action is irreversible.

Default Value:

When a new keyvault is created, both the parameters `enableSoftDelete` and `enablePurgeProtection` are set to `null` disabling both the features.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-soft-delete-cli
2. https://blogs.technet.microsoft.com/kv/2017/05/10/azure-key-vault-recovery-options/

CIS Controls:

Version 7

10 Data Recovery Capabilities
Data Recovery Capabilities

8.5 Enable role-based access control (RBAC) within Azure Kubernetes Services (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that RBAC is enabled on all Azure Kubernetes Services Instances

Rationale:

Azure Kubernetes Services has the capability to integrate Azure Active Directory users and groups into Kubernetes RBAC controls within the AKS Kubernetes API Server. This should be utilized to enable granular access to Kubernetes resources within the AKS clusters supporting RBAC controls not just of the overarching AKS instance but also the individual resources managed within Kubernetes.

Audit:

Azure Console

1. Go to Kubernetes Services
2. For each Kubernetes Services instance, click on Automation Script.
3. Ensure that each variable "enableRBAC" is set to true.

Azure Command Line Interface 2.0
Ensure that the output of the below command is not empty or null.

```
az aks show --name <AKS Instance Name> --query enableRbac --resource-group
<Resource Group Name> --subscription <Subscription ID>
```

Remediation:

WARNING: This setting cannot be changed after AKS deployment, cluster will require recreation.

Impact:

If RBAC is not enabled, the granularity of permissions granted to Kubernetes resources is diminished presenting more permissions than needed to users requiring access to Kubernetes resources in AKS.

Default Value:

By default, RBAC is enabled.

References:

1. https://docs.microsoft.com/en-us/azure/aks/aad-integrationhttps://kubernetes.io/docs/reference/access-authn-authz/rbac/https://docs.microsoft.com/en-us/cli/azure/aks?view=azure-cli-latest#az-aks-list

CIS Controls:

Version 7

4 Controlled Use of Administrative Privileges
Controlled Use of Administrative Privileges

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

9 AppService

This section covers security recommendations for Azure AppService.

9.1 Ensure App Service Authentication is set on Azure App Service (Scored)

Profile Applicability:

- Level 1

Description:

Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching the API app, or authenticate those that have tokens before they reach the API 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.

Audit:

Using Console:

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 / Authorization`
5. Ensure that `App Service Authentication` set to `On`

Using Command line:
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:

Using Console:

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 / Authorization`
5. Set `App Service Authentication` to `On`
6. Choose other parameters as per your requirement and Click on Save

Using Command Line:
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 false
```

Impact:

When it's enabled, every incoming HTTP request passes through it before being handled by the application code. So that an extra level of authentication process will be added to HTTP requests made to the app.

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

CIS Controls:

Version 7

16 Account Monitoring and Control
Account Monitoring and Control

9.2 Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service (Scored)

Profile Applicability:

- Level 1

Description:

Azure Web Apps allows sites to run under both HTTP and HTTPS by default. Web 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 request to HTTPS ports. HTTPS uses the SSL/TLS protocol to provide a secure connection, which is both encrypted and authenticated. So it is important to support HTTPS for the security benefits.

Audit:

Using Console:

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. Ensure that `HTTPS Only` set to `On` under `Protocol Settings`

Using Command line:
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 TTPS-only traffic value is set to `On`.

Remediation:

Using Console:

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. Set `HTTPS Only` to `On` under `Protocol Settings` section

Using Command Line:
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=false
```

Impact:

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

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://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl#enforce-https

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

9.3 Ensure web app is using the latest version of TLS encryption (Scored)

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:

Using Console:

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. Ensure that `Minimum TLS Version` set to `1.2` under `Protocol Settings`

Using Command line:
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 latest now).`

Remediation:

Using Console:

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. Set `Minimum TLS Version` to `1.2` under `Protocol Settings` section

Using Command Line:
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
```

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

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

9.4 Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Scored)

Profile Applicability:

- Level 1

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.

Audit:

Using Console:

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. Ensure that `Incoming client certificates` set to `On` under `Protocol Settings`

Using Command line:
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`.

Remediation:

Using Console:

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. Set `Incoming client certificates` to `On` under `Protocol Settings` section

Using Command Line:
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.

CIS Controls:

Version 7

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

9.5 Ensure that Register with Azure Active Directory is enabled on App Service (Scored)

Profile Applicability:

- Level 1

Description:

Managed service identity in App Service makes the app more secure by eliminating secrets from the app, such as credentials in the connection strings. When registering with Azure Active Directory in the app service, the app will connect to other Azure services securely without the need of username 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:

Using Console:

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under the `Setting` section, Click on `Identity`
5. Ensure that `Status` set to `On`

Using Command line:
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.

Remediation:

Using Console:

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. Set `Status` to `On`

Using Command Line:
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>
```

References:

1. https://docs.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-connect-msi

CIS Controls:

Version 7

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.

9.6 Ensure that '.Net Framework' version is the latest, if used as a part of the web app (Not Scored)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for .Net Framework software either due to security flaws or to include additional functionality. Using the latest .Net framework version for web apps is recommended in order to to take advantage of security fixes, if any, and/or new functionalities of the latest version.

Rationale:

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

Audit:

Using Console:

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 `Application settings`
5. Ensure that `.NET Framework version` set to latest version available under `General settings`

Using Command line:
To check .NET Framework version for an existing app, run the following command,

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

The output should return latest available version of .Net framework.

Remediation:

Using Console:

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 `Application settings`
5. Set `.NET Framework version` to latest version available under `General settings`

Using Command Line:
To see the list of supported runtimes:

```
az webapp list-runtimes | grep aspnet
```

To set latest .NET Framework version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--net-framework-version <VERSION>
```

Use .NET Framework as, 'v4.0' for .NET 4.6 and 'v3.0' for .NET 3.5.

Default Value:

By default, the latest .Net Framework version will be chosen when creating a new app using the command-line tool or Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings

CIS Controls:

Version 7

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.

9.7 Ensure that 'PHP version' is the latest, if used to run the web app (Not Scored)

Profile Applicability:

- Level 1

Description:

Periodically newer versions are released for PHP software either due to security flaws or to include additional functionality. Using the latest PHP version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.

Rationale:

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

Audit:

Using Console:

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 `Application settings`
5. Ensure that `PHP version` set to latest version available under `General settings`

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

The output should return the latest available version of PHP.
NOTE: No action is required, If the output is empty as PHP is not used by your web app.

Remediation:

Using Console:

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 `Application settings`
5. Set `PHP version` to latest version available under `General settings`

NOTE: No action is required If `PHP version` is set to `Off` as PHP is not used by your web app.
Using Command Line:
To see the list of supported runtimes:

```
az webapp list-runtimes | grep php
```

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>
--php-version <VERSION>
```

Default Value:

By default, PHP 5.6 version will be used when creating a new app using the command-line tool or the Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings

CIS Controls:

Version 7

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.

9.8 Ensure that 'Python version' is the latest, if used to run the web app (Not Scored)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest Python version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.

Rationale:

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

Audit:

Using Console:

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 `Application settings`
5. Ensure that `Python version` set to the latest version available under `General settings`

NOTE: No action is required, If `Python version` is set to `Off` as Python is not used by your web app.
Using Command line:
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 pythonVersion
```

The output should return the latest available version of Python.
NOTE: No action is required, If the output is empty as Python is not used by your web app.

Remediation:

Using Console:

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 `Application settings`
5. Set `Python version` to latest version available under `General settings`

NOTE: No action is required, If `Python version` is set to `Off` as Python is not used by your web app.
Using Command Line:
To see the list of supported runtimes:

```
az webapp list-runtimes | grep python
```

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>
--python-version <VERSION>
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings

CIS Controls:

Version 7

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.

9.9 Ensure that 'Java version' is the latest, if used to run the web app (Not Scored)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for Java software either due to security flaws or to include additional functionality. Using the latest Java version for web apps is recommended in order to take advantage of security fixes, if any, and/or new functionalities of the newer version.

Rationale:

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

Audit:

Using Console:

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 `Application settings`
5. Ensure that `Java version` set to the latest version available under `General settings`

NOTE: No action is required If `Java version` is set to `Off` as Java is not used by your web app.
Using Command line:
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 javaVersion
```

The output should return the latest available version of Java.
NOTE: No action is required If no output for above command as Java is not used by your web app.

Remediation:

Using Console:

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 `Application settings`
5. Under `General settings`, Set `Java version` to latest version available
6. Set `Java minor version` to latest version available
7. Set `Java web container` to the latest version of web container available

NOTE: No action is required If `Java version` is set to `Off` as Java is not used by your web app.
Using Command Line:
To see the list of supported runtimes:

```
az webapp list-runtimes | grep java
```

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

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--java-version '1.8' --java-container 'Tomcat' --java-container-version
'<VERSION>'
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings

CIS Controls:

Version 7

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.

9.10 Ensure that 'HTTP Version' is the latest, if used to run the web app (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

HTTP 2.0 has additional performance improvements 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.

Audit:

Using Console:

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 `Application settings`
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.
Using Command line:
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 TTPS-only traffic value is set to `On`.

Remediation:

Using Console:

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 `Application settings`
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.
Using Command Line:
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
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings

CIS Controls:

Version 7

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.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Identity and Access Management**		
1.1	Ensure that multi-factor authentication is enabled for all privileged users (Not Scored)	☐	☐
1.2	Ensure that multi-factor authentication is enabled for all non-privileged users (Not Scored)	☐	☐
1.3	Ensure that there are no guest users (Scored)	☐	☐
1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Not Scored)	☐	☐
1.5	Ensure that 'Number of methods required to reset' is set to '2' (Not Scored)	☐	☐
1.6	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to "0" (Not Scored)	☐	☐
1.7	Ensure that 'Notify users on password resets?' is set to 'Yes' (Not Scored)	☐	☐
1.8	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' (Not Scored)	☐	☐
1.9	Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Not Scored)	☐	☐
1.10	Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No' (Not Scored)	☐	☐
1.11	Ensure that 'Users can register applications' is set to 'No' (Not Scored)	☐	☐
1.12	Ensure that 'Guest user permissions are limited' is set to 'Yes' (Not Scored)	☐	☐
1.13	Ensure that 'Members can invite' is set to 'No' (Not Scored)	☐	☐
1.14	Ensure that 'Guests can invite' is set to 'No' (Not Scored)	☐	☐
1.15	Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes' (Not Scored)	☐	☐
1.16	Ensure that 'Self-service group management enabled' is set to 'No' (Not Scored)	☐	☐
1.17	Ensure that 'Users can create security groups' is set to 'No' (Not Scored)	☐	☐
1.18	Ensure that 'Users who can manage security groups' is set to 'None' (Not Scored)	☐	☐
1.19	Ensure that 'Users can create Office 365 groups' is set to 'No' (Not Scored)	☐	☐

1.20	Ensure that 'Users who can manage Office 365 groups' is set to 'None' (Not Scored)	☐	☐
1.21	Ensure that 'Enable "All Users" group' is set to 'Yes' (Not Scored)	☐	☐
1.22	Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' (Not Scored)	☐	☐
1.23	Ensure that no custom subscription owner roles are created (Scored)	☐	☐
2	**Security Center**		
2.1	Ensure that standard pricing tier is selected (Scored)	☐	☐
2.2	Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' (Scored)	☐	☐
2.3	Ensure ASC Default policy setting "Monitor System Updates" is not "Disabled" (Scored)	☐	☐
2.4	Ensure ASC Default policy setting "Monitor OS Vulnerabilities" is not "Disabled" (Scored)	☐	☐
2.5	Ensure ASC Default policy setting "Monitor Endpoint Protection" is not "Disabled" (Scored)	☐	☐
2.6	Ensure ASC Default policy setting "Monitor Disk Encryption" is not "Disabled" (Scored)	☐	☐
2.7	Ensure ASC Default policy setting "Monitor Network Security Groups" is not "Disabled" (Scored)	☐	☐
2.8	Ensure ASC Default policy setting "Monitor Web Application Firewall" is not "Disabled" (Scored)	☐	☐
2.9	Ensure ASC Default policy setting "Enable Next Generation Firewall(NGFW) Monitoring" is not "Disabled" (Scored)	☐	☐
2.10	Ensure ASC Default policy setting "Monitor Vulnerability Assessment" is not "Disabled" (Scored)	☐	☐
2.11	Ensure ASC Default policy setting "Monitor Storage Blob Encryption" is not "Disabled" (Scored)	☐	☐
2.12	Ensure ASC Default policy setting "Monitor JIT Network Access" is not "Disabled" (Scored)	☐	☐
2.13	Ensure ASC Default policy setting "Monitor Adaptive Application Whitelisting" is not "Disabled" (Scored)	☐	☐
2.14	Ensure ASC Default policy setting "Monitor SQL Auditing" is not "Disabled" (Scored)	☐	☐
2.15	Ensure ASC Default policy setting "Monitor SQL Encryption" is not "Disabled" (Scored)	☐	☐
2.16	Ensure that 'Security contact emails' is set (Scored)	☐	☐
2.17	Ensure that security contact 'Phone number' is set (Scored)	☐	☐
2.18	Ensure that 'Send email notification for high severity alerts' is set to 'On' (Scored)	☐	☐
2.19	Ensure that 'Send email also to subscription owners' is set to 'On' (Scored)	☐	☐

3	**Storage Accounts**		
3.1	Ensure that 'Secure transfer required' is set to 'Enabled' (Scored)	☐	☐
3.2	Ensure that storage account access keys are periodically regenerated (Not Scored)	☐	☐
3.3	Ensure Storage logging is enabled for Queue service for read, write, and delete requests (Not Scored)	☐	☐
3.4	Ensure that shared access signature tokens expire within an hour (Not Scored)	☐	☐
3.5	Ensure that shared access signature tokens are allowed only over https (Not Scored)	☐	☐
3.6	Ensure that 'Public access level' is set to Private for blob containers (Scored)	☐	☐
3.7	Ensure default network access rule for Storage Accounts is set to deny (Scored)	☐	☐
3.8	Ensure 'Trusted Microsoft Services' is enabled for Storage Account access (Not Scored)	☐	☐
4	**Database Services**		
4.1	Ensure that 'Auditing' is set to 'On' (Scored)	☐	☐
4.2	Ensure that 'AuditActionGroups' in 'auditing' policy for a SQL server is set properly (Scored)	☐	☐
4.3	Ensure that 'Auditing' Retention is 'greater than 90 days' (Scored)	☐	☐
4.4	Ensure that 'Advanced Data Security' on a SQL server is set to 'On' (Scored)	☐	☐
4.5	Ensure that 'Threat Detection types' is set to 'All' (Scored)	☐	☐
4.6	Ensure that 'Send alerts to' is set (Scored)	☐	☐
4.7	Ensure that 'Email service and co-administrators' is 'Enabled' (Scored)	☐	☐
4.8	Ensure that Azure Active Directory Admin is configured (Scored)	☐	☐
4.9	Ensure that 'Data encryption' is set to 'On' on a SQL Database (Scored)	☐	☐
4.10	Ensure SQL server's TDE protector is encrypted with BYOK (Use your own key) (Scored)	☐	☐
4.11	Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server (Scored)	☐	☐
4.12	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Scored)	☐	☐
4.13	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Scored)	☐	☐
4.14	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Scored)	☐	☐
4.15	Ensure server parameter 'log_disconnections' is set to 'ON' for	☐	☐

	PostgreSQL Database Server (Scored)		
4.16	Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server (Scored)	☐	☐
4.17	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Scored)	☐	☐
4.18	Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Scored)	☐	☐
4.19	Ensure that Azure Active Directory Admin is configured (Scored)	☐	☐
5	**Logging and Monitoring**		
5.1	**Configuring Log Profile**		
5.1.1	Ensure that a Log Profile exists (Scored)	☐	☐
5.1.2	Ensure that Activity Log Retention is set 365 days or greater (Scored)	☐	☐
5.1.3	Ensure audit profile captures all the activities (Scored)	☐	☐
5.1.4	Ensure the log profile captures activity logs for all regions including global (Scored)	☐	☐
5.1.5	Ensure the storage container storing the activity logs is not publicly accessible (Scored)	☐	☐
5.1.6	Ensure the storage account containing the container with activity logs is encrypted with BYOK (Use Your Own Key) (Scored)	☐	☐
5.1.7	Ensure that logging for Azure KeyVault is 'Enabled' (Scored)	☐	☐
5.2	**Monitoring using Activity Log Alerts**		
5.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment (Scored)	☐	☐
5.2.2	Ensure that Activity Log Alert exists for Create or Update Network Security Group (Scored)	☐	☐
5.2.3	Ensure that Activity Log Alert exists for Delete Network Security Group (Scored)	☐	☐
5.2.4	Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule (Scored)	☐	☐
5.2.5	Ensure that activity log alert exists for the Delete Network Security Group Rule (Scored)	☐	☐
5.2.6	Ensure that Activity Log Alert exists for Create or Update Security Solution (Scored)	☐	☐
5.2.7	Ensure that Activity Log Alert exists for Delete Security Solution (Scored)	☐	☐
5.2.8	Ensure that Activity Log Alert exists for Create or Update or Delete SQL Server Firewall Rule (Scored)	☐	☐
5.2.9	Ensure that Activity Log Alert exists for Update Security Policy (Scored)	☐	☐
6	**Networking**		
6.1	Ensure that RDP access is restricted from the internet	☐	☐

	(Scored)		
6.2	Ensure that SSH access is restricted from the internet (Scored)	☐	☐
6.3	Ensure no SQL Databases allow ingress 0.0.0.0/0 (ANY IP) (Scored)	☐	☐
6.4	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Scored)	☐	☐
6.5	Ensure that Network Watcher is 'Enabled' (Scored)	☐	☐
7	**Virtual Machines**		
7.1	Ensure that 'OS disk' are encrypted (Scored)	☐	☐
7.2	Ensure that 'Data disks' are encrypted (Scored)	☐	☐
7.3	Ensure that 'Unattached disks' are encrypted (Scored)	☐	☐
7.4	Ensure that only approved extensions are installed (Not Scored)	☐	☐
7.5	Ensure that the latest OS Patches for all Virtual Machines are applied (Not Scored)	☐	☐
7.6	Ensure that the endpoint protection for all Virtual Machines is installed (Not Scored)	☐	☐
8	**Other Security Considerations**		
8.1	Ensure that the expiration date is set on all keys (Scored)	☐	☐
8.2	Ensure that the expiration date is set on all Secrets (Scored)	☐	☐
8.3	Ensure that Resource Locks are set for mission critical Azure resources (Not Scored)	☐	☐
8.4	Ensure the key vault is recoverable (Scored)	☐	☐
8.5	Enable role-based access control (RBAC) within Azure Kubernetes Services (Scored)	☐	☐
9	**AppService**		
9.1	Ensure App Service Authentication is set on Azure App Service (Scored)	☐	☐
9.2	Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service (Scored)	☐	☐
9.3	Ensure web app is using the latest version of TLS encryption (Scored)	☐	☐
9.4	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Scored)	☐	☐
9.5	Ensure that Register with Azure Active Directory is enabled on App Service (Scored)	☐	☐
9.6	Ensure that '.Net Framework' version is the latest, if used as a part of the web app (Not Scored)	☐	☐
9.7	Ensure that 'PHP version' is the latest, if used to run the web app (Not Scored)	☐	☐
9.8	Ensure that 'Python version' is the latest, if used to run the web app (Not Scored)	☐	☐

9.9	Ensure that 'Java version' is the latest, if used to run the web app (Not Scored)	☐	☐
9.10	Ensure that 'HTTP Version' is the latest, if used to run the web app (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version	Ticket #
2/15/2019	1.1.0	DELETE - 3.2 and 3.6 - Ensure that 'Storage... - Rules are no longer valid or do not require	6185
2/15/2019	1.1.0	UPDATE - 2.17 Ensure that security contact - Not digitally signed warning	6224
2/15/2019	1.1.0	UPDATE - 5.1.2 Ensure that Activity Log... - Retention Days set to 0 to allow indefinite retention	6559
2/15/2019	1.1.0	UPDATE - 2.14 - Security Policy option name 'SQL auditing & Threat detection' is longer valid	6560
2/15/2019	1.1.0	UPDATE - Ensure audit profile captures all the activities - Remediation CLI change	6705
2/15/2019	1.1.0	UPDATE - Ensure log profile captures activity...- audit and remediation steps	6706
2/15/2019	1.1.0	UPDATE - 8.4 Keyvault is recoverable - audit and remediation CLI update	6737
2/15/2019	1.1.0	DELETE - Section 4.2 - Redundancy of Controls when intent has already addressed in 4.1	6778
2/15/2019	1.1.0	ADD - SQL Servers (4.1): Ensure that Audit Action Group in auditing policy for a server is set properly	6779
2/15/2019	1.1.0	UPDATE - Section 4: All recommendations change Azure Portal/Console Audit and Remediation Steps except 4.1.9 and 4.1.10	6781
2/15/2019	1.1.0	UPDATE - 4.1.2 thru 4.1.7 - Changes required in Level and/or Scoring	6789
2/15/2019	1.1.0	UPDATE - 4.1.1 Ensure that 'Auditing' is set to 'On' (SQL Server) - Description and notes updated	6790
2/15/2019	1.1.0	UPDATE - 4.2.6 `TDE' on Database - Clarified wording and implementation process	6795
2/15/2019	1.1.0	UPDATE - 4.1.6 `Email Service and co-Administrators' - Update Default value	6796
2/15/2019	1.1.0	DELETE - 7.1 Ensure that VM agent is installed	6802
2/15/2019	1.1.0	UPDATE - 6.3 SQL server Firewall Policy - does 0.0.0.0 means public access or Azure IP range	6803

2/15/2019	1.1.0	UPDATE - 6.3 SQL server Firewall Policy can be overridden by DB Firewall policy	6804
2/15/2019	1.1.0	UPDATE - 2.12 - JIT Network Access - Not a free service - Making it Level 2 to be aligned with 2.1 Pricing tier `Standard`	6810
2/15/2019	1.1.0	UPDATE - 2.13 Adaptive Application Controls - Making it Level 2 to be aligned with 2.1 Pricing tier `Standard`	6811
2/15/2019	1.1.0	DELETE - 3.6 Ensure that 'Storage service encryption' is set to Enabled for File Service	6812
2/15/2019	1.1.0	UPDATE - 4.8 Threat Detection Retention - Add case 0 : Indefinite Retention	6813
2/15/2019	1.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update or Delete...-title/rationale/description changed	6850
2/15/2019	1.1.0	DELETE - Ensure that Activity Log Alert exists for Delete SQL Server...5.2.9	6851
2/15/2019	1.1.0	ADD - Ensure that 'Unattached disks' are encrypted	6871
2/15/2019	1.1.0	UPDATE - Azure Security Center: Audit and Remediation console procedure changed	6874
2/15/2019	1.1.0	UPDATE - Ensure that the expiration date is set on all keys - Audit & Remediation Update	6920
2/15/2019	1.1.0	UPDATE - Ensure that the expiration date is set on all Secrets - Audit & Remediation Update	6921
2/15/2019	1.1.0	ADD - Propose 'Ensure 'Trusted Microsoft Services' is enabled for Storage Account access'	7079
2/15/2019	1.1.0	UPDATE- Ensure that 'Auditing' Retention is 'greater than 90 days' - Audit & Remediation Steps Update	7245
2/15/2019	1.1.0	ADD - Section for App Services Recommendations	7401
2/15/2019	1.1.0	UPDATE - Ensure that 'Members can invite' is set to 'No' - wording fix for Rationale	7407
2/15/2019	1.1.0	UPDATE - Section 2 - Azure Security Center changes to audit and remediation in all recommendations	7479
2/15/2019	1.1.0	UPDATE - SQL Service - Rename Section to Database Services	7559
2/15/2019	1.1.0	ADD - Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database	7566
2/15/2019	1.1.0	ADD - Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server	7567
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	7572

2/15/2019	1.1.0	ADD - Ensure server parameter 'log_connections' is set to 'ON' for Azure Database for PostgreSQL server	7573
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	7575
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server	7576
2/15/2019	1.1.0	ADD - Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	7578
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	7579
2/15/2019	1.1.0	UPDATE - Section 1 - Multiple recommendations changed to Not Scored	7673
2/15/2019	1.1.0	UPDATE - 3.5 Ensure that shared access signature tokens are allowed only - scoring change	7687
2/15/2019	1.1.0	UPDATE - section 9 multiple recommendations - Scoring status changed to Not Scored	7688
2/15/2019	1.1.0	Update - mapping of V7 Critical Controls on all recommendations	7703
2/15/2019	1.1.0	UPDATE - Section 2 recommendations - Audit and Remediation Portal Steps (Edit setting -> Edit settings)	7741
2/15/2019	1.1.0	UPDATE - Ensure that 'Send email notification for high severity alerts' is - Update Title, Audit, Remediation steps	7742
2/15/2019	1.1.0	UPDATE - Ensure server parameter 'connection_throttling' is set to 'ON'... - updated rational	7878
2/15/2019	1.1.0	UPDATE - Monitoring using Activity Log Alerts - audit CLI : Remove GET GET	7880
2/15/2019	1.1.0	UPDATE - Section 5.2 - Update all Audit CLIs to filter out only desired alert rule	7932
2/15/2019	1.1.0	UPDATE - Section 4 multiple recommendations - changed to Advanced Data Security	7954
2/15/2019	1.1.0	UPDATE - Ensure ASC Default policy setting "Monitor System Updates" - Minor Correction in Audit Procedure	7993
2/20/2018	1.0.0	Initial Release	