CIS Benchmarks

CIS Microsoft Azure Foundations

v1.0.0 - 02-20-2018

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

Terms of Use 1
Overview 7
Intended Audience 7
Consensus Guidance 7
Typographical Conventions 8
Scoring Information 8
Profile Definitions 9
Acknowledgements 10
Recommendations 11
1 Identity and Access Management 11
1.1 Ensure that multi-factor authentication is enabled for all privileged users (Scored) 11
1.2 Ensure that multi-factor authentication is enabled for all non-privileged users (Scored) 14
1.3 Ensure that there are no guest users (Scored) 17
1.4 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Scored) 19
1.5 Ensure that 'Number of methods required to reset' is set to '2' (Scored) 21
1.6 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Scored) 23
1.7 Ensure that 'Notify users on password resets?' is set to 'Yes' (Scored) 25
1.8 Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' (Scored) 27
1.9 Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Scored) 29
1.10 Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No' (Scored) 31
1.11 Ensure that 'Users can register applications' is set to 'No' (Scored) 33
1.12 Ensure that 'Guest users permissions are limited' is set to 'Yes' (Scored) 35
1.13 Ensure that 'Members can invite' is set to 'No' (Scored) 37
1.14 Ensure that 'Guests can invite' is set to 'No' (Scored) 39

1.15 Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes' (Scored) 41
1.16 Ensure that 'Self-service group management enabled' is set to 'No' (Scored) 43
1.17 Ensure that 'Users can create security groups' is set to 'No' (Scored) 45
1.18 Ensure that 'Users who can manage security groups' is set to 'None' (Scored) 47
1.19 Ensure that 'Users can create Office 365 groups' is set to 'No' (Scored) 49
1.20 Ensure that 'Users who can manage Office 365 groups' is set to 'None' (Scored) 51
1.21 Ensure that 'Enable "All Users" group' is set to 'Yes' (Scored) 53
1.22 Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' (Scored) 55
1.23 Ensure that no custom subscription owner roles are created (Scored) 57
2 Security Center 59
2.1 Ensure that standard pricing tier is selected (Scored) 59
2.2 Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' (Scored) 61
2.3 Ensure that 'System updates' is set to 'On' (Scored) 64
2.4 Ensure that 'Security Configurations' is set to 'On' (Scored) 67
2.5 Ensure that 'Endpoint protection' is set to 'On' (Scored) 70
2.6 Ensure that 'Disk encryption' is set to 'On' (Scored) 73
2.7 Ensure that 'Network security groups' is set to 'On' (Scored) 76
2.8 Ensure that 'Web application firewall' is set to 'On' (Scored) 79
2.9 Ensure that 'Next generation firewall' is set to 'On' (Scored) 82
2.10 Ensure that 'Vulnerability assessment' is set to 'On' (Scored) 85
2.11 Ensure that 'Storage Encryption' is set to 'On' (Scored) 88
2.12 Ensure that 'JIT Network Access' is set to 'On' (Scored) 91
2.13 Ensure that 'Adaptive Application Controls' is set to 'On' (Scored) 94
2.14 Ensure that 'SQL auditing & Threat detection' is set to 'On' (Scored) 97
2.15 Ensure that 'SQL Encryption' is set to 'On' (Scored) 100
2.16 Ensure that 'Security contact emails' is set (Scored) 103
2.17 Ensure that security contact 'Phone number' is set (Scored) 106
2.18 Ensure that 'Send me emails about alerts' is set to 'On' (Scored) 109

2.19 Ensure that 'Send email also to subscription owners' is set to 'On' (Scored) ..112
3 Storage Accounts ..115
3.1 Ensure that 'Secure transfer required' is set to 'Enabled' (Scored) ..115
3.2 Ensure that 'Storage service encryption' is set to Enabled for Blob Service (Scored) ..117
3.3 Ensure that storage account access keys are periodically regenerated (Not Scored) ..119
3.4 Ensure that shared access signature tokens expire within an hour (Not Scored) ..121
3.5 Ensure that shared access signature tokens are allowed only over https (Scored) ..123
3.6 Ensure that 'Storage service encryption' is set to Enabled for File Service (Scored) ..125
3.7 Ensure that 'Public access level' is set to Private for blob containers (Scored).127
4 SQL Services..129
4.1 SQL Servers..130
4.1.1 Ensure that 'Auditing' is set to 'On' (Scored) ..130
4.1.2 Ensure that 'Threat Detection' is set to 'On' (Scored) ..133
4.1.3 Ensure that 'Threat Detection types' is set to 'All' (Scored) ..135
4.1.4 Ensure that 'Send alerts to' is set (Scored) ..137
4.1.5 Ensure that 'Email service and co-administrators' is 'Enabled' (Scored) ..139
4.1.6 Ensure that 'Auditing' Retention is 'greater than 90 days' (Scored) ..141
4.1.7 Ensure that 'Threat Detection' Retention is 'greater than 90 days' (Scored) .143
4.1.8 Ensure that Azure Active Directory Admin is configured (Scored) ..145
4.2 SQL Databases ..148
4.2.1 Ensure that 'Auditing' is set to 'On' (Scored) ..148
4.2.2 Ensure that 'Threat Detection' is set to 'On' (Scored) ..150
4.2.3 Ensure that 'Threat Detection types' is set to 'All' (Scored) ..152
4.2.4 Ensure that 'Send alerts to' is set (Scored) ..154
4.2.5 Ensure that 'Email service and co-administrators' is 'Enabled' (Scored) ..156
4.2.6 Ensure that 'Data encryption' is set to 'On' (Scored) ..158
4.2.7 Ensure that 'Auditing' Retention is 'greater than 90 days' (Scored) ..160

4.2.8 Ensure that 'Threat' Retention is 'greater than 90 days' (Scored) 162
5 Logging and Monitoring 164
5.1 Ensure that a Log Profile exists (Scored) 164
5.2 Ensure that Activity Log Retention is set 365 days or greater (Scored) 166
5.3 Ensure that Activity Log Alert exists for Create Policy Assignment (Scored) 168
5.4 Ensure that Activity Log Alert exists for Create or Update Network Security Group (Scored) 170
5.5 Ensure that Activity Log Alert exists for Delete Network Security Group (Scored) 172
5.6 Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule (Scored) 174
5.7 Ensure that Activity Log Alert exists for Delete Network Security Group Rule (Scored) 176
5.8 Ensure that Activity Log Alert exists for Create or Update Security Solution (Scored) 178
5.9 Ensure that Activity Log Alert exists for Delete Security Solution (Scored) 180
5.10 Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Scored) 182
5.11 Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Scored) 184
5.12 Ensure that Activity Log Alert exists for Update Security Policy (Scored) 186
5.13 Ensure that logging for Azure KeyVault is 'Enabled' (Scored) 188
6 Networking 190
6.1 Ensure that RDP access is restricted from the internet (Scored) 190
6.2 Ensure that SSH access is restricted from the internet (Scored) 192
6.3 Ensure that SQL server access is restricted from the internet (Scored) 194
6.4 Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Scored) 196
6.5 Ensure that Network Watcher is 'Enabled' (Scored) 198
7 Virtual Machines 200
7.1 Ensure that VM agent is installed (Scored) 200
7.2 Ensure that 'OS disk' are encrypted (Scored) 202

7.3 Ensure that 'Data disks' are encrypted (Scored) 204
7.4 Ensure that only approved extensions are installed (Not Scored) 206
7.5 Ensure that the latest OS Patches for all Virtual Machines are applied (Not Scored) 208
7.6 Ensure that the endpoint protection for all Virtual Machines is installed (Not Scored) 210
8 Other Security Considerations 212
8.1 Ensure that the expiry date is set on all Keys (Scored) 212
8.2 Ensure that the expiry date is set on all Secrets (Scored) 214
8.3 Ensure that Resource Locks are set for mission critical Azure resources (Not Scored) 216
Appendix: Summary Table 218
Appendix: Change History 222

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 on 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 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:

Author
Pravin Goyal , Cavirin Systems, Inc.
Prabhu Angadi Security Content Author (Compliance | Configuration | Checklist)
Parag Patil

Contributor
Gururaj Pandurangi
Pravin Kulkarni
Ben Layer , Tripwire, Inc
Pierre Gronau
Felix Simmons
Jonathan Trull , Microsoft
Shamir Charania
Jordan Rakoske GSEC, GCWN

Recommendations

1 Identity and Access Management

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

1.1 Ensure that multi-factor authentication is enabled for all privileged users (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/Microsof
t.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/Microsof
t.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:

5.6 Use Multi-factor Authentication For All Administrative Access
Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

1.2 Ensure that multi-factor authentication is enabled for all non-privileged users (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/Microsof
t.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:

16.11 Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

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 such guest users. Guest users are typically added out of your employee on-boarding/off-boarding process and could potentially be lying there unnoticed 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:

16 Account Monitoring and Control
Account Monitoring and Control

1.4 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

Remembering Multi-Factor Authentication for devices and browsers allows you to give users 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 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 MFA is not bypassed.

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 would require performing 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:

16.11 Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

1.5 Ensure that 'Number of methods required to reset' is set to '2' (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that two alternate forms of identification are needed before allowing 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 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, `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:

16 Account Monitoring and Control
Account Monitoring and Control

1.6 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (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 goes 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, `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:

16 Account Monitoring and Control
Account Monitoring and Control

1.7 Ensure that 'Notify users on password resets?' is set to 'Yes' (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that the 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:

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' (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 inspect such an activity and confirm.

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:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.9 Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Scored)

Profile Applicability:

- Level 2

Description:

Require administrators to provide consent for the apps before use.

Rationale:

Until you are running Azure Active Directory as an identity provider for third-party applications, do not allow users to use the identity outside of your cloud environment. User's profile information contains private information such as phone number and email address 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.10 Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No' (Scored)

Profile Applicability:

- Level 2

Description:

Require administrators to provide consent for the apps before use.

Rationale:

Until you are running Azure Active Directory as an identity provider for third-party applications, do not allow users to use the identity outside of your cloud environment. User's profile information contains private information such as phone number and email address 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.11 Ensure that 'Users can register applications' is set to 'No' (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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.12 Ensure that 'Guest users permissions are limited' is set to 'Yes' (Scored)

Profile Applicability:

- Level 2

Description:

Limit guest user permissions.

Rationale:

Limiting guest access ensures that the guest accounts do not have permission for certain directory tasks, such as enumerate 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:

16 Account Monitoring and Control
Account Monitoring and Control

1.13 Ensure that 'Members can invite' is set to 'No' (Scored)

Profile Applicability:

- Level 2

Description:

Restrict invitation through administrators only.

Rationale:

Restricting invitation through administrators ensures that only authorized accounts have access to cloud resources. This helps to maintain 'Need to Know' and 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.14 Ensure that 'Guests can invite' is set to 'No' (Scored)

Profile Applicability:

- Level 2

Description:

Restrict guest invitations.

Rationale:

Restricting invitation through administrators ensures that only authorized accounts have access to cloud resources. This helps to maintain 'Need to Know' and 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.15 Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes' (Scored)

Profile Applicability:

- Level 1

Description:

Restrict access to Azure AD administration portal to administrators only.

Rationale:

Azure AD administrative portal has sensitive data. You should restrict all non-administrators 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.16 Ensure that 'Self-service group management enabled' is set to 'No' (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). Until your business requires this day-to-day delegation to some users, it is good to disable self-service group management.

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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.17 Ensure that 'Users can create security groups' is set to 'No' (Scored)

Profile Applicability:

- Level 2

Description:

Restrict security group creation to administrators only.

Rationale:

When Users can create security groups is enabled, all users in your directory are allowed to create new security groups and add members to these groups. Until your business require this day-to-day delegation, you should restrict security group creation 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.18 Ensure that 'Users who can manage security groups' is set to 'None' (Scored)

Profile Applicability:

- Level 2

Description:

Restrict security group management to administrators only.

Rationale:

Restricting security group management to administrators only does not allow users to make changes to security groups. This ensures that security 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 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.19 Ensure that 'Users can create Office 365 groups' is set to 'No' (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 there is no proliferation of such groups. Appropriate groups should be created and managed by the administrator and such 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.20 Ensure that 'Users who can manage Office 365 groups' is set to 'None' (Scored)

Profile Applicability:

- Level 2

Description:

Restrict Office 365 group management to administrators only.

Rationale:

Restricting Office 365 group management to administrators only does not allow users to make 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:

5.1 Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

1.21 Ensure that 'Enable "All Users" group' is set to 'Yes' (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 your directory. For example, you can grant all users in your directory access to a SaaS application by assigning access for the All Users dedicated group to this application. This ensures that you can have a common policy created for all users and need not restrict permissions individually.

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:

16.9 Configure Account Access Centrally
Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

1.22 Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' (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 that 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:

5.6 Use Multi-factor Authentication For All Administrative Access
Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

16.11 Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

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

Profile Applicability:

- Level 2

Description:

Do not create custom roles with subscription ownership. It is recommended to use the principle of least privilege, assigning only needed privileges 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, to begin with, the least necessary permission, and add permissions 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:

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

2 Security Center

This section covers security recommendations that you should follow to set various security policies on your 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 respective alerts if any security violation is found. They do not actually enforce security settings by themselves. You should follow these alerts and remediate wherever possible.

2.1 Ensure that standard pricing tier is selected (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

Enabling the Standard pricing tier allows for further 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 to alter in turn
4. Select the `Pricing tier` blade
5. Review the chosen pricing tier

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 Security Center`
2. Select `Security policy` blade
3. Select subscription to alter
4. Select the `Pricing tier` blade
5. Select `Standard`
6. Select `Save`

Impact:

Choosing the Standard 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

CIS Controls:

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 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, and endpoint protection and provides alerts.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.logCollection'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on each subscription
4. Click on `Data Collection`
5. Set `Automatic provisioning of monitoring agent` to `On`

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
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

4.3 Vulnerability Scanning In Authenticated Mode
Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.

2.3 Ensure that 'System updates' is set to 'On' (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 `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `System updates` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.patch'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Set `System updates` to `On`

Azure Command Line Interface 2.0

Use the below command to set `System updates` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

Impact:

None

Default Value:

By default, `System updates` is set to `On`.

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

2.4 Ensure that 'Security Configurations' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable OS vulnerabilities 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 `Security Center`
2. Click on `Security Policy`
3. Select an Azure Subscription
4. Click on `Security Policy`
5. Ensure that `Security Configurations` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.baseline'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Select an Azure Subscription
4. Click on `Security Policy`

5. Set `Security Configurations` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Security Configurations` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

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 the team takes remediatory actions for the recommendations will allow for appropriate level of security controls.

Default Value:

By default, `Security Configurations` is set to `On`.

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

3.1 Establish Standard Secure Configurations For OS And Software
Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

2.5 Ensure that 'Endpoint protection' is set to 'On' (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 `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Endpoint protection` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.antimalware'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`

5. Set `Endpoint protection` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Endpoint protection` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
{
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
}
```

Impact:

None

Default Value:

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

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

8.1 Deploy Automated Endpoint Protection Tools
Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

2.6 Ensure that 'Disk encryption' is set to 'On' (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 to enhance data protection at rest.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Disk encryption` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.diskEncryption'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Set `Disk encryption` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Disk encryption` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
        {
            "properties" :
            {
              "logCollection": "On",
              "recommendations": {
                "patch": "On",
                "baseline": "On",
                "antimalware": "On",
                "diskEncryption": "On",
                "acls": "On",
                "nsgs": "On",
                "waf": "On",
                "sqlAuditing": "On",
                "sqlTde": "On",
                "ngfw": "On",
                "vulnerabilityAssessment": "On",
                "storageEncryption": "On",
                "jitNetworkAccess": "On",
                "appWhitelisting": "On"
              }
            }
        }
```

Impact:

None

Default Value:

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

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

14.5 Encrypt At Rest Sensitive Information
Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

2.7 Ensure that 'Network security groups' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable Network security groups 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 is 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 `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Network security groups` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.nsgs'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Set `Network security groups` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Network security groups` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
        {
            "properties" :
            {
              "logCollection": "On",
              "recommendations": {
                "patch": "On",
                "baseline": "On",
                "antimalware": "On",
                "diskEncryption": "On",
                "acls": "On",
                "nsgs": "On",
                "waf": "On",
                "sqlAuditing": "On",
                "sqlTde": "On",
                "ngfw": "On",
                "vulnerabilityAssessment": "On",
                "storageEncryption": "On",
                "jitNetworkAccess": "On",
                "appWhitelisting": "On"
              }
            }
        }
```

Impact:

None

Default Value:

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

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

12 Boundary Defense
Boundary Defense

2.8 Ensure that 'Web application firewall' is set to 'On' (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 `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Web application firewall` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.waf'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Set `Web application firewall` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Web application firewall` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
        {
            "properties" :
            {
              "logCollection": "On",
              "recommendations": {
                "patch": "On",
                "baseline": "On",
                "antimalware": "On",
                "diskEncryption": "On",
                "acls": "On",
                "nsgs": "On",
                "waf": "On",
                "sqlAuditing": "On",
                "sqlTde": "On",
                "ngfw": "On",
                "vulnerabilityAssessment": "On",
                "storageEncryption": "On",
                "jitNetworkAccess": "On",
                "appWhitelisting": "On"
              }
            }
        }
```

Impact:

None

Default Value:

By default, `Web application firewall` is set to `On`.

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

18.2 Deploy And Configure Web Application Firewalls
Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

2.9 Ensure that 'Next generation firewall' is set to 'On' (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 discover deployments for which a next generation firewall is recommended and enable you to provision a virtual appliance.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Next generation firewall` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.ngfw'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`

5. Set `Next generation firewall` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Next generation firewall` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
        {
            "properties" :
            {
              "logCollection": "On",
              "recommendations": {
                "patch": "On",
                "baseline": "On",
                "antimalware": "On",
                "diskEncryption": "On",
                "acls": "On",
                "nsgs": "On",
                "waf": "On",
                "sqlAuditing": "On",
                "sqlTde": "On",
                "ngfw": "On",
                "vulnerabilityAssessment": "On",
                "storageEncryption": "On",
                "jitNetworkAccess": "On",
                "appWhitelisting": "On"
              }
            }
        }
```

Impact:

None

Default Value:

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

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

12.3 Deploy Network-based IDS Sensors on DMZ Systems
Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

2.10 Ensure that 'Vulnerability assessment' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable Vulnerability assessment recommendations for virtual machines.

Rationale:

When this setting is enabled, it recommends that you install a vulnerability assessment solution on your VM.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Vulnerability assessment` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq
'.properties.recommendations.vulnerabilityAssessment'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`

5. Set `Vulnerability assessment` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Vulnerability assessment` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

Impact:

None

Default Value:

By default, `Vulnerability assessment` is set to `On`.

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

4.1 Weekly Automated Vulnerability Scanning
Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

2.11 Ensure that 'Storage Encryption' is set to 'On' (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 `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Storage Encryption` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.storageEncryption'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Set `Storage Encryption` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Storage Encryption` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

Impact:

None

Default Value:

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

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

14.5 Encrypt At Rest Sensitive Information
Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

2.12 Ensure that 'JIT Network Access' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable JIT Network Access for virtual machines.

Rationale:

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

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `JIT Network Access` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.jitNetworkAccess'
```

Remediation:

Azure Console

1. Go to `Security Center`

2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Set `JIT Network Access` to `On`

Azure Command Line Interface 2.0

Use the below command to set `JIT Network Access` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

Impact:

None

Default Value:

By default, `JIT Network Access` is set to `On`.

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

12 Boundary Defense
Boundary Defense

2.13 Ensure that 'Adaptive Application Controls' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable adaptive application controls.

Rationale:

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

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `Adaptive Application Controls` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.appWhitelisting'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription

4. Click on `Security policy`
5. Set `Adaptive Application Controls` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Adaptive Application Controls` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

Impact:

None

Default Value:

By default, `Adaptive Application Controls` is set to `On`.

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

CIS Controls:

2.2 Deploy Application Whitelisting

Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

2.14 Ensure that 'SQL auditing & Threat detection' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable SQL auditing & Threat detection recommendations.

Rationale:

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

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `SQL auditing & Threat detection` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.sqlAuditing'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Set `SQL auditing & Threat detection` to `On`

Azure Command Line Interface 2.0

Use the below command to set `SQL auditing & Threat detection` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

Impact:

None

Default Value:

By default, `SQL auditing & Threat detection` is set to `On`.

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

CIS Controls:

18.7 Use Standard Database Hardening Templates
For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

2.15 Ensure that 'SQL Encryption' is set to 'On' (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 your Azure SQL Database, associated backups, and transaction log files. Even if your data is breached, it will not be readable.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`
5. Ensure that `SQL Encryption` 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.recommendations.sqlTde'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Security policy`

5. Set `SQL Encryption` to `On`

Azure Command Line Interface 2.0

Use the below command to set `SQL Encryption` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-preview -d@"input.json"'
```

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

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      }
    }
    }
```

Impact:

None

Default Value:

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

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

Notes:

Excluding any of the entries in `input.json` disables the specific setting by default.

CIS Controls:

14.5 Encrypt At Rest Sensitive Information
Sensitive information stored on systems shall be encrypted at rest and require 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 provided security contact in case its security team finds that your resources are compromised. This ensures that you are aware of any potential compromise and you can timely mitigate the risk.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq
'.properties.securityContactConfiguration.securityContactEmails'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`

3. Click on the security policy subscription
4. Click on `Email notifications`
5. Set a valid email address for the security contact

Azure Command Line Interface 2.0

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

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-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.

```
{
        "properties": {
                "logCollection": "On",
                "recommendations": {
                        "patch": "On",
                        "baseline": "On",
                        "antimalware": "On",
                        "diskEncryption": "On",
                        "acls": "On",
                        "nsgs": "On",
                        "waf": "On",
                        "sqlAuditing": "On",
                        "sqlTde": "On",
                        "ngfw": "On",
                        "vulnerabilityAssessment": "On",
                        "storageEncryption": "On",
                        "jitNetworkAccess": "On",
                        "appWhitelisting": "On"
                },
                "securityContactConfiguration": {
                        "securityContactEmails": [
                                "<validEmailAddress>"
                        ],
                        "securityContactPhone": "<phoneNumber>",
                        "areNotificationsOn": true,
                        "sendToAdminOn": true
                }
        }
}
```

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

Notes:

Excluding any of the entries in recommendations block in `input.json` disables the specific setting by default.

CIS Controls:

19 Incident Response and Management
Incident Response and 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 provided security contact in case its security team finds that your resources are compromised. This ensures that you are aware of any potential compromise and you can timely mitigate the risk.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq
'.properties.securityContactConfiguration.securityContactPhone'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`

3. Click on the security policy subscription
4. Click on `Email notifications`
5. Set a valid security contact Phone number

Azure Command Line Interface 2.0

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

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-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.

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      },
      "securityContactConfiguration": {
          "securityContactEmails": [
            "<validEmailAddress>"
          ],
          "securityContactPhone": "<phoneNumber>",
          "areNotificationsOn": true,
          "sendToAdminOn": true
        }
    }
    }
```

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

Notes:

Excluding any of the entries in recommendations block in `input.json` disables the specific setting by default.

CIS Controls:

19 Incident Response and Management
Incident Response and Management

2.18 Ensure that 'Send me emails about alerts' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable security alerts emailing to security contact.

Rationale:

Enabling security alerts emailing ensures that you receive the security alert emails from Microsoft. This ensures that you are aware of any potential security issues and you can timely mitigate the risk.

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Email notifications`
5. Ensure that `Send me emails about 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq
'.properties.securityContactConfiguration.areNotificationsOn'
```

Remediation:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on the security policy subscription

4. Click on `Email notifications`
5. Set `Send me emails about alerts` to `On`

Azure Command Line Interface 2.0

Use the below command to set `Send me emails about alerts` to `On`.

```
az account get-access-token --query
"{subscripton: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/po
licies/default?api-version=2015-06-01-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.

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      },
      "securityContactConfiguration": {
          "securityContactEmails": [
            "<validEmailAddress>"
          ],
          "securityContactPhone": "<phoneNumber>",
          "areNotificationsOn": true,
          "sendToAdminOn": true
        }
    }
    }
```

Impact:

None

Default Value:

By default, `Send me emails about alerts` is not set.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

Notes:

Excluding any of the entries in recommendations block in `input.json` disables the specific setting by default.

CIS Controls:

19 Incident Response and Management
Incident Response and Management

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

Profile Applicability:

- Level 1

Description:

Enable security alerts emailing to subscription owners.

Rationale:

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

Audit:

Azure Console

1. Go to `Security Center`
2. Click on `Security Policy`
3. Click on 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
"{subscripton: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/po
licies?api-version=2015-06-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq
'.properties.securityContactConfiguration.sendToAdminOn'
```

Remediation:

Azure Console

1. Go to `Security Center`

2. Click on `Security Policy`
3. Click on the security policy subscription
4. Click on `Email notifications`
5. Set `Send email also to subscription owners` to `On`

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
"{subscripton: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/po
licies/default?api-version=2015-06-01-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.

```
    {
    "properties" :
    {
      "logCollection": "On",
      "recommendations": {
        "patch": "On",
        "baseline": "On",
        "antimalware": "On",
        "diskEncryption": "On",
        "acls": "On",
        "nsgs": "On",
        "waf": "On",
        "sqlAuditing": "On",
        "sqlTde": "On",
        "ngfw": "On",
        "vulnerabilityAssessment": "On",
        "storageEncryption": "On",
        "jitNetworkAccess": "On",
        "appWhitelisting": "On"
      },
      "securityContactConfiguration": {
          "securityContactEmails": [
            "<validEmailAddress>"
          ],
          "securityContactPhone": "<phoneNumber>",
          "areNotificationsOn": true,
          "sendToAdminOn": true
        }
    }
    }
```

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

CIS Controls:

19 Incident Response and Management
Incident Response and Management

3 Storage Accounts

This section covers security recommendations that you should follow to set storage account policies on your Azure Subscription. An Azure storage account provides a unique namespace to store and access your 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 your storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access your storage accounts, you must connect using HTTPs. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When you are 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:

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

3.2 Ensure that 'Storage service encryption' is set to Enabled for Blob Service (Scored)

Profile Applicability:

- Level 1

Description:

Enable data encryption at rest for blobs.

Rationale:

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.

Audit:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Encryption` under `BLOB SERVICE`
3. Ensure that `Storage service encryption` is set to `Enabled`

Azure Command Line Interface 2.0

In the output of the below command ensure the `Storage Account Name` has its associated `BLOB SERVICE` encryption is not null.

```
az storage account list --query [*].[name,encryption.services.blob.enabled]
```

Remediation:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Encryption` under `BLOB SERVICE`
3. Set `Storage service encryption` to `Enabled`

Azure Command Line Interface 2.0

Use the below command to enable the `Encryption` for `Storage Accounts BLOB SERVICE`

```
az storage account update --name <storageAccountName> --resource-group
<resourceGroupName> --set encryption.services.blob.enabled=true
```

Impact:

None

Default Value:

By default, `Storage service encryption` is set to Disabled for Blob service.

References:

1. https://docs.microsoft.com/en-us/azure/storage/storage-security-guide#encryption-at-rest
2. https://docs.microsoft.com/en-in/azure/storage/blobs/storage-java-how-to-use-blob-storage#overview
3. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_list
4. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_update

CIS Controls:

14.5 Encrypt At Rest Sensitive Information
Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

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

Profile Applicability:

- Level 1

Description:

Regenerate storage account access keys periodically.

Rationale:

When you create a storage account, 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 to these keys could be undermined.

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 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 your storage account access keys.

Impact:

Regenerating your access keys can affect services in Azure as well as your own 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:

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

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. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time. This time should be set to as low as possible and preferably should be within an hour.

Audit:

You cannot currently audit SAS token expiry times created historically. Until Microsoft makes token expiry time as 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, expiry 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:

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

3.5 Ensure that shared access signature tokens are allowed only over https (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. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time. It is recommended to allow such access requests over https protocol only.

Audit:

You cannot currently audit SAS token protocols created historically. Until Microsoft makes SAS transfer protocols as a setting rather than a token creation parameter, this recommendation would 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:

14.2 Encrypt All Sensitive Information Over Less-trusted Networks
All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.

3.6 Ensure that 'Storage service encryption' is set to Enabled for File Service (Scored)

Profile Applicability:

- Level 1

Description:

Enable data encryption at rest for file service.

Rationale:

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in its datacenters, and automatically decrypts it for you as you access it.

Audit:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Encryption` under `FILE SERVICE`
3. Ensure that `Storage service encryption` is set to `Enabled`

Azure Command Line Interface 2.0

In the output of the below command ensure the `Storage Account` name has its associated `FILE SERVICE` encryption is not null.

```
az storage account list --query [*].[name,encryption.services.file.enabled]
```

Remediation:

Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Encryption` under `FILE SERVICE`
3. Set `Storage service encryption` to `Enabled`

Azure Command Line Interface 2.0

Use the below command to enable the Encryption for `Storage Accounts FILE SERVICE`.

```
az storage account update --name <storageAccountName> --resource-group
<resourceGroupName> --set encryption.services.file.enabled=true
```

Impact:

None

Default Value:

By default, `Storage service encryption` is set to `Disabled for file service`.

References:

1. https://docs.microsoft.com/en-us/azure/storage/storage-security-guide#encryption-at-rest
2. https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share

CIS Controls:

14.5 Encrypt At Rest Sensitive Information
Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

3.7 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:

You can enable anonymous, public read access to a container and its blobs in Azure Blob storage. By doing so, you can grant read-only access to these resources without sharing your account key, and without requiring a shared access signature. It is recommended to not provide anonymous access to blob containers until and unless it is strongly desired. You should use shared access signature token 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:

You will have to manage access using shared access signatures.

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:

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

4 SQL Services

This section covers security recommendations that you should follow to set SQL Services policies on your Azure Subscription.

4.1 SQL Servers

This section covers security recommendations that you should follow to set SQL Server policies on your Azure Subscription.

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

Profile Applicability:

- Level 1

Description:

Enable auditing on SQL Servers.

Rationale:

The Azure platform allows you to create a SQL server 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 tracks database events and writes them to an audit log in your Azure storage account. It also helps you 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 & Threat Detection`
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 & Threat Detection`
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

CIS Controls:

14.6 Enforce Detailed Audit Logging For Sensitive Information
Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

4.1.2 Ensure that 'Threat Detection' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable threat detection on SQL Servers.

Rationale:

SQL Threat Detection 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 Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing & Threat Detection`
4. Ensure that `Threat Detection` 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 `Auditing & Threat Detection`
4. Set `Threat Detection` to `On`

Azure PowerShell

Enable `ThreatDetection` for a SQL Server:

```
Set-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name> -NotificationRecipientsEmails <Email Ids for
notification recipients> -EmailAdmins $True -StorageAccountName <storage
account name>
```

Impact:

None

Default Value:

By default, `Threat Detection` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection
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:

12.3 Deploy Network-based IDS Sensors on DMZ Systems

Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

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

Profile Applicability:

- Level 1

Description:

Enable all types of threat detection on SQL Servers.

Rationale:

Enabling all threat detection types, you are protected 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 `Auditing & Threat Detection`
4. 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 `Auditing & Threat Detection`
4. 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-database-threat-detection
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:

12.3 Deploy Network-based IDS Sensors on DMZ Systems

Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

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

Profile Applicability:

- Level 1

Description:

Provide the email address to which alerts will be sent upon detection of anomalous activities 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 `Auditing & Threat Detection`
4. 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 `Auditing & Threat Detection`
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-database-threat-detection
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:

19 Incident Response and Management
Incident Response and Management

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

Profile Applicability:

- Level 1

Description:

Enable service and co-administrators to receive security alerts from 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 `Auditing & Threat Detection`
4. 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 `Auditing & Threat Detection`
4. 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 not set.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection
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:

19 Incident Response and Management
Incident Response and Management

4.1.6 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 & Threat Detection`
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 & Threat Detection`
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:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

4.1.7 Ensure that 'Threat Detection' Retention is 'greater than 90 days' (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Threat Detection Logs can be used to check for suspected attack attempts and breaches on a SQL server with known attack signatures.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing & Threat Detection`
4. In `Threat Detection` Section, Ensure `Retention (days)` setting `greater than 90 days`

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 `RetentionInDays` is set to `more than 90`.

Remediation:

Azure Console

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

3. Click on `Auditing & Threat Detection`
4. In Threat Detection Section, Set `Retention (days)` setting `greater than 90 days`
5. Click `OK`
6. Click `Save`

Azure PowerShell

For each Server, set the retention policy for more than 90 days

```
set-AzureRmSqlServerThreatDetectionPolicy -ResourceGroupName <resource group
name> -ServerName <server name> -RetentionInDays <Number of Days to retain
the audit logs>
```

Impact:

None

Default Value:

By default, SQL Server Threat Detection Retention is set to `0`.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection
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:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

4.1.8 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 of connecting to Microsoft Azure SQL Database and SQL Data Warehouse by using identities in Azure Active Directory (Azure AD). With Azure AD authentication, you can centrally manage the identities of database users and other Microsoft services 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:

16.9 Configure Account Access Centrally

Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.

4.2 SQL Databases

This section covers security recommendations that you should follow to set SQL Database policies on your Azure Subscription.

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

Profile Applicability:

- Level 1

Description:

Enable auditing on SQL databases.

Rationale:

Auditing tracks database events and writes them to an audit log in your Azure storage account. It also helps you 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 databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Ensure that `Auditing` is set to `On`

Azure Command Line Interface 2.0

Ensure the below command output is `Enabled`

```
az sql db audit-policy show --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --query 'state'
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each DB instance

3. Click on `Auditing & Threat Detection`
4. Set `Auditing` to `On`

Azure Command Line Interface 2.0

Use the below command to set SQL Databases `Auditing` to `On`

```
az sql db audit-policy update --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --state Enabled
```

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing

CIS Controls:

14.6 Enforce Detailed Audit Logging For Sensitive Information
Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.

4.2.2 Ensure that 'Threat Detection' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Enable threat detection on SQL databases.

Rationale:

SQL Threat Detection 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 Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat.

Audit:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Ensure that `Threat Detection` is set to `On`

Azure Command Line Interface 2.0

Ensure the output of the below command contains `Enabled`

```
az sql db threat-policy show --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --query 'state'
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Set `Threat Detection` to `On`

Azure Command Line Interface 2.0

Use below command to set SQL Databases `Threat Detection` to `On`

```
az sql db threat-policy update --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --state Enabled
```

Impact:

None

Default Value:

By default, `Threat Detection` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection

CIS Controls:

12.3 Deploy Network-based IDS Sensors on DMZ Systems

Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

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

Profile Applicability:

- Level 1

Description:

Enable all types of threat detection on SQL databases.

Rationale:

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

Audit:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Ensure that `Threat Detection types` is set to `All`

Azure Command Line Interface 2.0

Ensure the below command. output is `All` or `Empty String`

```
az sql db threat-policy show --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --query 'disabledAlerts'
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Set `Threat Detection types` to `All`

Azure Command Line Interface 2.0

Use the below command to ensure `SQL Databases Threat Detection types` is set to `All`.

```
az sql db threat-policy update --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --disabled-alerts All
```

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection

CIS Controls:

12.3 Deploy Network-based IDS Sensors on DMZ Systems
Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.

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

Profile Applicability:

- Level 1

Description:

Provide the email address to which alerts will be sent upon detection of anomalous activities on SQL databases.

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 databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Ensure that `Send alerts to` is set as appropriate

Azure Command Line Interface 2.0

Ensure the below command output contains valid email addresses.

```
az sql db threat-policy show --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --query emailAddresses
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Set `Send alerts to` as appropriate

Azure Command Line Interface 2.0

Use the below command to set `SQL Databases Send Alerts to` is set to valid email addresses, by providing semicolon separated list of email addresses.

```
az sql db threat-policy update --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --email-addresses <semi colon separated list of
email addresses>
```

Impact:

None

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection

CIS Controls:

19 Incident Response and Management
Incident Response and Management

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

Profile Applicability:

- Level 1

Description:

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

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 databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Ensure that `Email service and co-administrators` is `Enabled`

Azure Command Line Interface 2.0

Ensure the below command output is `Enabled`

```
az sql db threat-policy show --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --query emailAccountAdmins
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Auditing & Threat Detection`
4. Enable `Email service and co-administrators`

Azure Command Line Interface 2.0

Use the below command to enable `SQL Databases Email service and co-administrators`.

```
az sql db threat-policy update --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --email-account-admins Enabled
```

Impact:

None

Default Value:

By default, `Email service and co-administrators` is not set.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection

CIS Controls:

19 Incident Response and Management
Incident Response and Management

4.2.6 Ensure that 'Data encryption' is set to 'On' (Scored)

Profile Applicability:

- Level 1

Description:

Encrypt database.

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:

14.5 Encrypt At Rest Sensitive Information

Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

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

Profile Applicability:

- Level 1

Description:

SQL Database 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 databases`
2. For each database
3. Click on `Auditing & Threat Detection`
4. Select `Storage Details`
5. Ensure `Retention (days)` setting `greater than 90 days`

Azure Command Line Interface 2.0

Ensure the output for the below command is `greater than 90`.

```
az sql db audit-policy show --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --query 'retentionDays'
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each database
3. Click on `Auditing & Threat Detection`
4. Select `Storage Details`
5. Set `Retention (days)` setting `greater than 90 days`
6. Select `OK`
7. Select `Save`

Azure Command Line Interface 2.0

Use the below command to set SQL Databases Auditing Retention to `greater than 90 days`

```
az sql db audit-policy update --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --retention-days <NumberOfDays>
```

Impact:

None

Default Value:

By default, SQL Database 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/cli/azure/sql/db/audit-policy?view=azure-cli-latest#az_sql_db_audit_policy_show

CIS Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

4.2.8 Ensure that 'Threat' Retention is 'greater than 90 days' (Scored)

Profile Applicability:

- Level 1

Description:

SQL Database Threat Retention should be configured to be greater than 90 days.

Rationale:

Threat 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 databases`
2. For each database, click on `Auditing & Threat Detection`
3. Ensure that `Auditing` is set to `ON`
4. Click on `Storage details`
5. Ensure that the `Retention (Days)` is set to `90 or above`.

Azure Command Line Interface 2.0

Ensure the below command output is `greater than 90 days`.

```
az sql db threat-policy show --resource-group <resourceGroup> --server
<serverName> --name <dbName> --query retentionDays
```

Remediation:

Azure Console

1. Go to `SQL databases`
2. For each database, click on `Auditing & Threat Detection`
3. Ensure that `Auditing` is set to `ON`
4. Click on `Storage details`
5. Configure an appropriate `Storage account` and `Retention (Days)` to `90 or above`.

Azure Command Line Interface 2.0

Use the below command to set `SQL Databases Threat Detection` retention days to `more than 90 days`.

```
az sql db threat-policy update --resource-group <resourceGroupName> --server
<serverName> --name <dbName> --retention-days <numberOfDays>
```

References:

1. https://docs.microsoft.com/en-us/cli/azure/sql/db/threat-policy?view=azure-cli-latest#az_sql_db_threat_policy_update
2. https://docs.microsoft.com/en-us/cli/azure/sql/db/threat-policy?view=azure-cli-latest#az_sql_db_threat_policy_show

Notes:

No portal(UI) steps are available

CIS Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

5 Logging and Monitoring

This section covers security recommendations that you should follow to set logging and monitoring policies on your Azure Subscription.

5.1 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 your Activity Log is exported. By default, activity logs are retained only for 90 days. It is thus recommended to define a log profile using which you could export the logs and store them for a longer duration for analyzing security activities within your 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:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

5.2 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 your Activity Log is exported and retained. Since the average time to detect a breach is 210 days, it is recommended to retain your activity log 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 greater`

Azure Command Line Interface 2.0

Ensure the below command output contains `days` set `365` and `enabled` set to `true`.

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

Remediation:

Azure Console

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

Note: Setting the `Retention (days)` to `0` retains the data forever.

Impact:

None

Default Value:

By default, Activity Log Retention is `disabled`.

References:

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

CIS Controls:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

5.3 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 gives insight into privilege assignment and may reduce the time it takes to detect a breach or misuse of information.

Audit:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Create Policy Assignment`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Authorization/policyAssignments/write"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select `Event category Administrative`
5. Select Operation name `Create policy assignment`
6. Set a subscription and action group for alerts
7. Select `Save`

Azure Command Line Interface 2.0

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

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Authorization/policyAssignments/write -a
<actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax
`/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

5.4 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 network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Create or Update Network Security Group`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Network/networkSecurityGroups/write"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Create or Update Network Security Group`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

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

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/write -a <actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log?view=azure-cli-latest

CIS Controls:

5.4 Log Administrative User Addition And Removal

Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

5.5 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 network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Delete Network Security Group`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Network/networkSecurityGroups/delete"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Delete Network Security Group`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Delete Network Security Group`

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/delete -a <actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax `/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5.4 Log Administrative User Addition And Removal

Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

5.6 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. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Create or Update Security Rule`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Network/networkSecurityGroups/securityRules/write"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Create or Update Security Rule`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

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

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/securityRules/write -a
<actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax `/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5.4 Log Administrative User Addition And Removal

Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

5.7 Ensure that Activity Log Alert exists for 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. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Delete Security Rule`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Network/networkSecurityGroups/securityRules/delete"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Delete Security Rule`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Delete Security Rule`

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/securityRules/delete -a
<actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax
`/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5.4 Log Administrative User Addition And Removal
Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

5.8 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. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Create or Update Security Solutions`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Security/securitySolutions/write"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Create or Update Security Solutions`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

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

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/write -a <actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax `/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5.4 Log Administrative User Addition And Removal

Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

5.9 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. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Delete Security Solutions`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Security/securitySolutions/delete"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Delete Security Solutions`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Delete Security Solutions`

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/delete -a <actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax
`/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5.4 Log Administrative User Addition And Removal
Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

5.10 Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Scored)

Profile Applicability:

- Level 1

Description:

Create an Activity Log Alert for the Create or Update SQL Server Firewall Rule event.

Rationale:

Monitoring for Create or Update SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Create/Update server firewall rule`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Sql/servers/firewallRules/write"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Create/Update server firewall rule`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Create/Update server firewall rule`

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/write -a <actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax `/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5 Controlled Use of Administration Privileges

Controlled Use of Administration Privileges

5.11 Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Scored)

Profile Applicability:

- Level 1

Description:

Create an Activity Log Alert for the Delete SQL Server Firewall Rule event.

Rationale:

Monitoring for 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. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Delete server firewall rule`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Sql/servers/firewallRules/delete"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Delete server firewall rule`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Delete server firewall rule`

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/delete -a <actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax `/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

11 Secure Configurations for Network Devices such as Firewalls, Routers and switches
Secure Configurations for Network Devices such as Firewalls, Routers and switches

5.12 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 the Security Policy and may reduce the time it takes to detect suspicious activity.

Audit:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Check for Activity Log Alert for Operation name `Update security policy`

Azure Command Line Interface 2.0

Ensure the below command's output is not empty.

```
az monitor activity-log alert list --resource-group <resourceGroupName> --
query [*].condition | jq '.|.[].allOf[] | select(.equals |
contains("Microsoft.Security/policies/write"))'
```

Remediation:

Azure Console

1. Go to `Alerts`
2. Select `Add activity log alert`
3. Set a name, subscription, and resource group in which to store activity log alerts
4. Select Event category `Administrative`
5. Select Operation name `Update Security Policy`
6. Set a subscription and action group for alerts
7. Select Save

Azure Command Line Interface 2.0

Use the below command to create an Activity Log Alert for `Update security policy`

```
az monitor activity-log alert create -n <activityLogAlertName> -g
<resourceGroupName> --condition category=Administrative and
operationName=Microsoft.Security/policies/write -a <actionGroup>
```

Impact:

None

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-alerts-portal No artifacts listed Add New Artifact Revision History Current Version 59 seconds ago Ben 10 modifications View Diff 2 minutes ago Ben 1 modification View Diff © 2017 v2.0.117 Tickets Discussions Changes Tickets for Ensure Activity Log Alert exists for Delete SQL Server Firewall Rule No tickets listed Create New Ticket
2. https://docs.microsoft.com/en-us/cli/azure/monitor/activity-log/alert?view=azure-cli-latest#az_monitor_activity_log_alert_create

Notes:

`actionGroup` is of the following syntax
`/subscriptions/{SubID}/resourceGroups/{ResourceGroup}/providers/microsoft.insights/actionGroups/{ActionGroup}`

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

5.13 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 your key vaults are accessed, and by whom enables an audit trail of interactions with your secrets, keys and certificates managed by Azure Keyvault. You can do this by enabling logging for Key Vault, which saves information in an Azure storage account that you provide. This creates a new container named insights-logs-auditevent automatically for your specified storage account, and you can use this same storage account 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:

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

6 Networking

This section covers security recommendations that you should follow to set networking policies on your 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 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 your virtual machine as a launch point for compromising other machines on your 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:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services 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 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 your virtual machine as a launch point for compromising other machines on your 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:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

6.3 Ensure that SQL server access is restricted from the internet (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that no SQL Databases allow ingress from the internet.

Rationale:

SQL Database includes a firewall to block access to unauthorized connections. After creating your SQL Database, you can specify which IP addresses can connect to your database. You can then define more granular IP addresses by referencing the range of addresses available from specific datacenters.

Allowing ingress for the IP range 0.0.0.0/0 (StartIp of 0.0.0.0 and EndIP of 0.0.0.0) allows open access to any/all traffic potentially making the SQL Database vulnerable to attacks.

Audit:

Azure Console

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall / Virtual Networks`
4. Ensure that the firewall rules exist, and no rule has

- Start IP of `0.0.0.0`
- and End 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` and `EndIpAddress` is not set to `0.0.0.0` or other combinations which allows access to wider public IP ranges.

Remediation:

Azure Console

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall / Virtual Networks`
4. Set firewall rules to limit access to only authorized connections

Azure PowerShell

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>"
```

Impact:

None

Default Value:

By default, no firewall rules are configured.

References:

1. https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-set-database-firewall-rule-azure-sql-database
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

CIS Controls:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

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 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 your 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:

6.3 Ensure Audit Logging Systems Are Not Subject To Loss (i.e. rotation/archive)
Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.

6.5 Ensure that Network Watcher is 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Enable Network Watcher for your Azure Subscriptions.

Rationale:

Network diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your 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:

12 Boundary Defense
Boundary Defense

7 Virtual Machines

This section covers security recommendations that you should follow to set virtual machine policies on your Azure Subscription.

7.1 Ensure that VM agent is installed (Scored)

Profile Applicability:

- Level 1

Description:

Install VM agent on Virtual Machines.

Rationale:

The VM agent must be installed on Azure virtual machines (VMs) in order to enable Azure Security center for data collection. Security Center collects data from your virtual machines (VMs) to assess their security state, provide security recommendations, and alert you to threats.

Audit:

Azure Console

1. Go to `Azure Security Center`
2. In the `Recommendations blade`, select `Enable VM Agent`
3. This opens the blade `VM Agent Is Missing Or Not Responding`
4. Review this list and ensure that there are no VMs that are missing the agent

Azure Command Line Interface 2.0

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

It should list `"virtualMachineExtensionType": "MicrosoftMonitoringAgent"` with `"provisioningState": "Succeeded"`.

Remediation:

Azure Console

1. Go to `Azure Security Center`
2. In the `Recommendations blade`, select `Enable VM Agent`

3. This opens the blade `VM Agent Is Missing Or Not Responding`
4. Follow instructions from Azure and install VM agent where missing

Impact:

None

Default Value:

By default, VM Agent is installed for VMs that are deployed from the Azure Marketplace.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-vm-agent
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection
3. https://azure.microsoft.com/en-us/blog/vm-agent-and-extensions-part-2/
4. https://docs.microsoft.com/en-us/cli/azure/vm/extension?view=azure-cli-latest#az_vm_extension_list

CIS Controls:

3.6 Implement Automated Configuration Monitoring System (i.e. Configuration Assessment Tools)
Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

7.2 Ensure that 'OS disk' are encrypted (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that OS disks (boot volumes) are encrypted, where possible.

Rationale:

Encrypting your 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:

14.5 Encrypt At Rest Sensitive Information
Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, in order to access the information.

7.3 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 your 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 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

CIS Controls:

14.5 Encrypt At Rest Sensitive Information
Sensitive information stored on systems shall be encrypted at rest and require 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 your 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 your virtual machine. Azure portal and community provide several such extensions. Your organization should carefully evaluate such extensions and ensure that only those that are approved for use are actually used.

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:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

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

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. Security Center also checks for the latest updates in Linux systems. If your VM is missing a system update, Security Center will recommend that you apply system updates.

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 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:

4.5 Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

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 your 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 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:

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

8 Other Security Considerations

This section covers security recommendations that you should follow to set general security and operational controls on your Azure Subscription.

8.1 Ensure that the expiry date is set on all Keys (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that all Keys in Azure Key Vault have an expiry 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 you rotate your keys in the key vault and set an explicit expiry 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. 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 is not empty or null.

```
az keyvault key list --vault-name <vaultName> --query
[*].[attributes.expires]
```

Remediation:

Azure Console

1. Go to `Key vaults`

2. For each Key vault, click on `Keys`.
3. 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 expiry times respectively. You would have to rotate your keys periodically at all places 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:

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

8.2 Ensure that the expiry date is set on all Secrets (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that all Secrets in Azure Key Vault have an expiry time set.

Rationale:

Azure Key Vault enables users to store and secrets within the Microsoft Azure environment. Secrets in 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 that you rotate your secrets in the key vault and set an explicit expiry 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. Ensure that each secret in the vault has `EXPIRATION DATE` set as appropriate

Azure Command Line Interface 2.0

Ensure the output of the below command is not empty or null.

```
az keyvault secret list --vault-name <vaultName> --query
[*].[attributes.expires]
```

Remediation:

Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Secrets`.
3. 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. You would have to rotate your secrets periodically at all places 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:

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

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 or changing of 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 you have an important resource in your 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, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level 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:

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

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 (Scored)	☐	☐
1.2	Ensure that multi-factor authentication is enabled for all non-privileged users (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' (Scored)	☐	☐
1.5	Ensure that 'Number of methods required to reset' is set to '2' (Scored)	☐	☐
1.6	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Scored)	☐	☐
1.7	Ensure that 'Notify users on password resets?' is set to 'Yes' (Scored)	☐	☐
1.8	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' (Scored)	☐	☐
1.9	Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Scored)	☐	☐
1.10	Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No' (Scored)	☐	☐
1.11	Ensure that 'Users can register applications' is set to 'No' (Scored)	☐	☐
1.12	Ensure that 'Guest users permissions are limited' is set to 'Yes' (Scored)	☐	☐
1.13	Ensure that 'Members can invite' is set to 'No' (Scored)	☐	☐
1.14	Ensure that 'Guests can invite' is set to 'No' (Scored)	☐	☐
1.15	Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes' (Scored)	☐	☐
1.16	Ensure that 'Self-service group management enabled' is set to 'No' (Scored)	☐	☐
1.17	Ensure that 'Users can create security groups' is set to 'No' (Scored)	☐	☐
1.18	Ensure that 'Users who can manage security groups' is set to 'None' (Scored)	☐	☐
1.19	Ensure that 'Users can create Office 365 groups' is set to 'No' (Scored)	☐	☐
1.20	Ensure that 'Users who can manage Office 365 groups' is set	☐	☐

	to 'None' (Scored)		
1.21	Ensure that 'Enable "All Users" group' is set to 'Yes' (Scored)	☐	☐
1.22	Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' (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 that 'System updates' is set to 'On' (Scored)	☐	☐
2.4	Ensure that 'Security Configurations' is set to 'On' (Scored)	☐	☐
2.5	Ensure that 'Endpoint protection' is set to 'On' (Scored)	☐	☐
2.6	Ensure that 'Disk encryption' is set to 'On' (Scored)	☐	☐
2.7	Ensure that 'Network security groups' is set to 'On' (Scored)	☐	☐
2.8	Ensure that 'Web application firewall' is set to 'On' (Scored)	☐	☐
2.9	Ensure that 'Next generation firewall' is set to 'On' (Scored)	☐	☐
2.10	Ensure that 'Vulnerability assessment' is set to 'On' (Scored)	☐	☐
2.11	Ensure that 'Storage Encryption' is set to 'On' (Scored)	☐	☐
2.12	Ensure that 'JIT Network Access' is set to 'On' (Scored)	☐	☐
2.13	Ensure that 'Adaptive Application Controls' is set to 'On' (Scored)	☐	☐
2.14	Ensure that 'SQL auditing & Threat detection' is set to 'On' (Scored)	☐	☐
2.15	Ensure that 'SQL Encryption' is set to 'On' (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 me emails about 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 service encryption' is set to Enabled for Blob Service (Scored)	☐	☐
3.3	Ensure that storage account access keys are periodically regenerated (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 (Scored)	☐	☐
3.6	Ensure that 'Storage service encryption' is set to Enabled for	☐	☐

	File Service (Scored)		
3.7	Ensure that 'Public access level' is set to Private for blob containers (Scored)	☐	☐
4	**SQL Services**		
4.1	**SQL Servers**		
4.1.1	Ensure that 'Auditing' is set to 'On' (Scored)	☐	☐
4.1.2	Ensure that 'Threat Detection' is set to 'On' (Scored)	☐	☐
4.1.3	Ensure that 'Threat Detection types' is set to 'All' (Scored)	☐	☐
4.1.4	Ensure that 'Send alerts to' is set (Scored)	☐	☐
4.1.5	Ensure that 'Email service and co-administrators' is 'Enabled' (Scored)	☐	☐
4.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days' (Scored)	☐	☐
4.1.7	Ensure that 'Threat Detection' Retention is 'greater than 90 days' (Scored)	☐	☐
4.1.8	Ensure that Azure Active Directory Admin is configured (Scored)	☐	☐
4.2	**SQL Databases**		
4.2.1	Ensure that 'Auditing' is set to 'On' (Scored)	☐	☐
4.2.2	Ensure that 'Threat Detection' is set to 'On' (Scored)	☐	☐
4.2.3	Ensure that 'Threat Detection types' is set to 'All' (Scored)	☐	☐
4.2.4	Ensure that 'Send alerts to' is set (Scored)	☐	☐
4.2.5	Ensure that 'Email service and co-administrators' is 'Enabled' (Scored)	☐	☐
4.2.6	Ensure that 'Data encryption' is set to 'On' (Scored)	☐	☐
4.2.7	Ensure that 'Auditing' Retention is 'greater than 90 days' (Scored)	☐	☐
4.2.8	Ensure that 'Threat' Retention is 'greater than 90 days' (Scored)	☐	☐
5	**Logging and Monitoring**		
5.1	Ensure that a Log Profile exists (Scored)	☐	☐
5.2	Ensure that Activity Log Retention is set 365 days or greater (Scored)	☐	☐
5.3	Ensure that Activity Log Alert exists for Create Policy Assignment (Scored)	☐	☐
5.4	Ensure that Activity Log Alert exists for Create or Update Network Security Group (Scored)	☐	☐
5.5	Ensure that Activity Log Alert exists for Delete Network Security Group (Scored)	☐	☐
5.6	Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule (Scored)	☐	☐
5.7	Ensure that Activity Log Alert exists for Delete Network Security Group Rule (Scored)	☐	☐

5.8	Ensure that Activity Log Alert exists for Create or Update Security Solution (Scored)	☐	☐
5.9	Ensure that Activity Log Alert exists for Delete Security Solution (Scored)	☐	☐
5.10	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Scored)	☐	☐
5.11	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Scored)	☐	☐
5.12	Ensure that Activity Log Alert exists for Update Security Policy (Scored)	☐	☐
5.13	Ensure that logging for Azure KeyVault is 'Enabled' (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 that SQL server access is restricted from the internet (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 VM agent is installed (Scored)	☐	☐
7.2	Ensure that 'OS disk' are encrypted (Scored)	☐	☐
7.3	Ensure that 'Data 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 expiry date is set on all Keys (Scored)	☐	☐
8.2	Ensure that the expiry date is set on all Secrets (Scored)	☐	☐
8.3	Ensure that Resource Locks are set for mission critical Azure resources (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
2/20/2018	1.0.0	Initial Release