

CIS Microsoft Azure Database Services Benchmark

v1.0.0 - 06-28-2024

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
Table of Contents	2
Overview	5
Intended Audience.....	6
Consensus Guidance	7
Typographical Conventions.....	8
Recommendation Definitions.....	9
Title.....	9
Assessment Status.....	9
Automated	9
Manual.....	9
Profile	9
Description.....	9
Rationale Statement	9
Impact Statement.....	10
Audit Procedure.....	10
Remediation Procedure.....	10
Default Value.....	10
References	10
CIS Critical Security Controls® (CIS Controls®).....	10
Additional Information.....	10
Profile Definitions	11
Acknowledgements	12
Recommendations	13
1 Introduction.....	13
1.1 Multiple Methods of Audit and Remediation.....	15
2 Azure Cache for Redis.....	17
2.1 Ensure 'Microsoft Entra Authentication' is 'Enabled' (Manual)	18
2.2 Ensure that 'Allow access only via SSL' is set to 'Yes' (Automated)	20
2.3 Ensure that 'Minimum TLS version' is set to TLS v1.2 (or higher) (Manual)	22
2.4 Ensure that 'Access Policies' are implemented and reviewed periodically (Manual)	24
2.5 Ensure that 'System Assigned Managed Identity' is set to 'On' (Manual)	26
2.6 Ensure that 'Public Network Access' is 'Disabled' (Manual)	28
3 Azure Cosmos DB	30
3.1 Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Automated)	31

3.2 Ensure That Private Endpoints Are Used Where Possible (Automated).....	34
3.3 Use Entra ID Client Authentication and Azure RBAC where possible. (Manual)	37
4 Azure Data Factory	39
5 Azure Database for MariaDB (Retiring)	40
6 Azure Database for MySQL	41
6.1 Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server (Automated)	42
6.2 Ensure 'TLS Version' is set to 'TLSV1.2' (or higher) for MySQL flexible Database Server (Automated)	44
6.3 Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server (Manual)	47
6.4 Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server (Manual)	49
7 Azure Database for PostgreSQL.....	51
7.1 Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated)	52
7.2 Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated)	54
7.3 Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Automated)	57
7.4 Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated).....	60
7.5 Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Automated).....	63
7.6 Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Automated)	66
7.7 Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Automated)	69
7.8 Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Single Server Only) (Automated).....	71
8 Azure Database Migration Service	74
9 Azure SQL (Reference).....	75
10 Azure SQL Database.....	76
10.1 Ensure that 'Auditing' is set to 'On' (Automated)	77
10.2 Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated) ...	81
10.3 Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated).....	85
10.4 Ensure that Microsoft Entra authentication is Configured for SQL Servers (Automated)	89
10.5 Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)	93
10.6 Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)	96
10.7 Ensure Public Network Access is Disabled (Manual).....	99
11 Azure SQL Edge.....	101
12 Azure SQL Managed Instance.....	102
13 SQL Server on Azure Virtual Machines	103
14 Table Storage (Reference).....	104
15 Azure Managed Instance for Apache Cassandra	105
16 Azure confidential ledger	106

<i>Appendix: Summary Table.....</i>	<i>107</i>
<i>Appendix: CIS Controls v7 IG 1 Mapped Recommendations.....</i>	<i>110</i>
<i>Appendix: CIS Controls v7 IG 2 Mapped Recommendations.....</i>	<i>111</i>
<i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations.....</i>	<i>113</i>
<i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i>	<i>115</i>
<i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations.....</i>	<i>116</i>
<i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations.....</i>	<i>117</i>
<i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations.....</i>	<i>119</i>
<i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i>	<i>121</i>

Overview

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

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches.
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches.

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

This benchmark - CIS Microsoft Azure Database Services Benchmark - will provide secure configuration recommendations for Azure products that Microsoft has categorized as “Database” services in the Azure Products Directory (<https://azure.microsoft.com/en-us/products#databases>).

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

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

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

Intended Audience

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

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

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

- **Level 2**

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

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

Acknowledgements

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

Contributor

Krishna Rayavaram

Ian McRee

Jim Cheng

Steve Johnson

Robert Burton

Recommendations

1 Introduction

Benchmark Approach:

The suggested approach for securing your cloud environment is to start with the CIS Microsoft Azure Foundations Benchmark found here: <https://www.cisecurity.org/benchmark/azure>. The CIS Foundations Benchmark provides prescriptive guidance for configuring a subset of Microsoft Azure Services with an emphasis on foundational, testable, and architecture agnostic settings for services including:

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

The Microsoft Azure Foundation Benchmark is what you should start with when setting up your Azure environment. It is also the foundation for which all other Azure service based benchmarks are built on so that as you grow your cloud presence and usage of the services offered you have the necessary guidance to securely configure your environment as it fits with your company's policy.

After configuring your environment to the CIS Microsoft Azure Foundations Benchmark, we suggest implementing the necessary configurations for the services utilized as defined in the associated product and service level benchmarks. The CIS Microsoft Azure Database Services Benchmark provides prescriptive guidance for configuring security options for the services within Azure's Databases category. The specific Azure Services in scope for this document include:

- Azure Cache for Redis
- Azure Cosmos DB
- Azure Data Factory
- Azure Database for MariaDB
- Azure Database for MySQL
- Azure Database for PostgreSQL
- Azure Database Migration Service
- Azure SQL
- Azure SQL Database
- Azure SQL Edge

- Azure SQL Managed Instance
- SQL Server on Azure Virtual Machines
- Table Storage
- Azure Managed Instance for Apache Cassandra
- Azure confidential ledger

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS Microsoft Azure Benchmarks, please register on CIS WorkBench at <https://workbench.cisecurity.org> and join the CIS Microsoft Azure Benchmarks community.

1.1 Multiple Methods of Audit and Remediation

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

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

Setting Up PowerShell and Azure CLI

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

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

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

The Azure CLI tool can be installed from the following location:

<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli>

For PowerShell, the following cmdlets are required:

1. Azure PowerShell: <https://docs.microsoft.com/en-us/powershell/azure/install-az-ps-msi?view=azps-8.2.0>
2. Microsoft Graph PowerShell: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/get-started?view=graph-powershell-1.0>

3. Azure AD PowerShell for Graph: <https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-2.0>
4. MS Online PowerShell: <https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0>

Authenticating with Azure CLI

Run the following command from either PowerShell or command prompt:

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

Authenticating with PowerShell

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

```
Connect-AzAccount -Subscription <subscription ID> -Tenant <Tenant ID>  
Connect-MgGraph  
Connect-MsolService  
Connect-AzureAD
```

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

2 Azure Cache for Redis

Azure Product Page: <https://azure.microsoft.com/en-us/products/cache/>

Azure Policy for Cache for Redis: <https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/policy-reference>

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

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

2.1 Ensure 'Microsoft Entra Authentication' is 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Ensuring that Microsoft Entra Authentication is 'Enabled' provides a natively integrated use of identities already defined with Microsoft Entra ID.

Rationale:

The use of a centralized Identity and Access Management (IAM) solution such as Microsoft Entra ID is highly recommended for all activity related to Identity, Authentication, Authorization, and Accountability.

Decentralized IAM – such as local authentication methods – may present additional vulnerability and introduce avoidable administrative complexity.

Impact:

Free tiers exist for the licensing of Microsoft Entra ID if required.

Audit:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, click on **Authentication**
5. Review the checkbox next to **Enable Microsoft Entra Authentication**

If the checkbox is **Checked**, the configuration for that instance is compliant.

Remediation:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, click on **Authentication**
5. **Check** the checkbox next to **Enable Microsoft Entra Authentication**





Default Value:

By default, Microsoft Entra Authentication is **Checked** during setup.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management>
2. <https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-azure-active-directory-for-authentication>

CIS Controls:

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

2.2 Ensure that 'Allow access only via SSL' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1

Description:

Setting 'Allow access only via SSL' to 'Yes' ensures that data in transit to and from Azure Cache for Redis is encrypted using TLS.

Rationale:

Data in transit which is not encrypted is vulnerable to attacks including adversary-in-the-middle (AITM or MITM), eavesdropping, or session hijack. These attacks can result in the compromise and exfiltration of data.

Impact:

No additional cost is required to implement this recommendation. Aside from expected network changes (no unencrypted communications), performance should not be impacted.

Audit:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, under Settings, click on **Advanced Settings**
5. Review the setting under **Allow access only via SSL**

If **Yes** is selected, the configuration for that instance is compliant.

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [22bee202-a82f-4305-9a2a-6d7f44d4dedb](#) - **Name:** 'Only secure connections to your Azure Cache for Redis should be enabled'

Remediation:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, under Settings, click on **Advanced Settings**
5. Select **Yes** under the **Allow access only via SSL** heading





Default Value:

By default, 'Allow access only via SSL' is set to 'Yes.'

References:

1. <https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-best-practices-development>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-cache-for-redis-security-baseline#microsoft-defender-for-cloud-monitoring-1>

CIS Controls:

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

2.3 Ensure that 'Minimum TLS version' is set to TLS v1.2 (or higher) (Manual)

Profile Applicability:

- Level 1

Description:

Setting the 'Minimum TLS version' helps reduce (but not eliminate) TLS protocol vulnerabilities by preventing the use of significantly outdated versions of TLS.

Rationale:

Older versions of the TLS protocol have demonstrated vulnerabilities and should be avoided where possible. While TLS Protocol Version 1.3 is the most recent and preferred version in cases where it is available, version 1.2 is most broadly available and implemented by vendors. When it is configured to avoid specific vulnerable features of the protocol, version 1.2 of TLS can provide a secure implementation.

Versions 1.0 and 1.1 of TLS are no longer considered secure. These versions should not be used or permitted where data integrity and confidentiality are required.

Impact:

This configuration setting should not result in any perceptible changes to cost or performance.

Audit:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance listed, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, under Settings, click on **Advanced Settings**
5. Review the setting under **Minimum TLS version**

If **1.2 (Recommended)** (or a higher version) is selected, the configuration for that instance is compliant.

Remediation:

From Azure Portal





1. Search for and open the **Azure Cache for Redis** service
2. For each instance listed, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, under Settings, click on **Advanced Settings**

5. Click the drop-down menu under **Minimum TLS version**
6. Select **1.2 (Recommended)** (higher versions are preferred when available)

References:

1. <https://www.rfc-editor.org/rfc/pdf/rfc8446.txt.pdf>
2. <https://nvd.nist.gov/vuln/detail/CVE-2016-0701>

CIS Controls:

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

2.4 Ensure that 'Access Policies' are implemented and reviewed periodically (Manual)

Profile Applicability:

- Level 2

Description:

Access Policies provide an Access Control List (ACL) functionality allowing administrators to define which identities or identity groups have access to what data and commands. This is an implementation of the Role Based Access Control (RBAC) concept and will require careful consideration to deploy and maintain.

Rationale:

Role Based Access Control (RBAC) using Access Control Lists (ACLs) is a method of implementing the principle of least privilege by ensuring that users and user groups with differing needs are presented with the privilege that fulfills their needs and any unnecessary access or functionality is prevented.

Impact:

Implementing RBAC for any system requires a careful analysis of 'who' needs access to the system, and 'what' privileges or functionality they need to perform. The time required to implement RBAC will increase based on the complexity and size of an environment.

If RBAC is deployed without careful analysis, it may prevent users from accessing data or functionality that they require from the system. Conversely, it may present privilege which is unnecessary and introduce vulnerability to a system.

Once RBAC has been deployed, there should be periodically scheduled access review. During the access review, all entries in the Access Control List and all identities are reviewed for fitness and necessity.

Audit:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, under Settings, click on **Data Access Configuration**
5. Click on the tab titled **Access Policies** and review the access policies for fitness and necessity.

Please note: No more specific definition can be presented here because the definitions of fitness and necessity are judgments that must be made by the administrators and security personnel with knowledge of the identities and functionality required of the system being evaluated.

Remediation:

No prescriptive remediation is available due to the specific and unique nature of implementing RBAC for any given system. Implementing RBAC for any system requires a careful analysis of 'who' needs access to the system, and 'what' privileges or functionality they require. The time required to implement RBAC will increase based on the complexity and size of an environment.

Default Value:

By default, no Access Policies exist.

References:

1. <https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-configure-role-based-access-control>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 <u>Define and Maintain Role-Based Access Control</u> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.7 <u>Enforce Access Control to Data through Automated Tools</u> Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

2.5 Ensure that 'System Assigned Managed Identity' is set to 'On' (Manual)

Profile Applicability:

- Level 1

Description:

System Assigned Managed Identities provide the Azure Cache for Redis instance with a unique account like a service principle but automatically assigned and managed by Azure. These identities are unique to the resource instance they are created for, and removed when the resource is deleted.

Rationale:

The System Assigned Managed Identity is authenticated with Entra ID, and allows for privileges required for the instance of Azure Cache for Redis to be granted or restricted using Azure Role Based Access Control (RBAC). Additionally, the managed identity provides a means for the Azure Cache for Redis instance to authenticate without storing credentials in code.

Audit:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, under Settings, click on **Identity**
5. Under the **System assigned** tab, ensure that **Status** is set to **On**.

If **Yes** is selected and **Object (principal) ID** is populated, the configuration for that instance is compliant.

Remediation:

From Azure Portal

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, under Settings, click on **Identity**
5. Under the **System assigned** tab, toggle the status to **On**
6. Click the **Save** button
7. In the pop-up dialog titled **Enable system assigned managed identity** that appears after clicking save, click the **Yes** button.



Default Value:

By default, System Assigned Managed Identity of **Off**.

References:

1. <https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-managed-identity>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

2.6 Ensure that 'Public Network Access' is 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Disabling public network access restricts the service from accessing public networks.

Rationale:

A secure network architecture requires carefully constructed network segmentation. Public Network Access tends to be overly permissive and introduces unintended vectors for threat activity.

Impact:

Some architectural consideration may be necessary to ensure that required network connectivity is still made available. No additional cost or performance impact is required to deploy this recommendation.

IMPORTANT NOTE: If Azure Cache for Redis has been deployed in a VNet, this recommendation cannot be implemented. See additional information below for more detail.

Audit:

From Azure Portal

NOTE: This procedure applies only to instances that are not using VNets.

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance
4. In the blade menu on the left, click on **Private Endpoint**
5. Review the button to the right of **+ Private Endpoint**

If the button is titled **enable public network access**, the configuration for that instance is currently disabled and compliant.

Remediation:

From Azure Portal

NOTE: A Private Endpoint must exist before the “Disable public network access” button allows the configuration change to be performed via Portal.

1. Search for and open the **Azure Cache for Redis** service
2. For each instance, repeat the remaining steps
3. Click on the name of the instance

4. In the blade menu on the left, click on **Private Endpoint**
5. Click the **Disable public network access** button.

Default Value:

By default Public Network Access is **Disabled** when creating an Azure Cache for Redis instance.







References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>
2. <https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-network-isolation>
3. <https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-private-link#how-can-i-change-my-private-endpoint-to-be-disabled-or-enabled-from-public-network-access>

Additional Information:

For Azure Cache for Redis instances deployed in classic VNets (Virtual Network injection), public network access cannot be disabled. In these cases, an equivalent control using restrictive Access Control Lists (ACLs) in Network Security Groups (NSGs) and/or Azure Firewall is recommended. If it is feasible, the Azure Cache for Redis instance can also be deleted and re-created with a new instance using Private Endpoints instead of VNets.

CIS Controls:

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

3 Azure Cosmos DB

This section covers security best practice recommendations for Azure Cosmos DB Database Servers.

Azure Product Page: <https://azure.microsoft.com/en-us/products/cosmos-db/>

3.1 Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Automated)

Profile Applicability:

- Level 2

Description:

Limiting your Cosmos DB to only communicate on whitelisted networks lowers its attack footprint.

Rationale:

Selecting certain networks for your Cosmos DB to communicate restricts the number of networks including the internet that can interact with what is stored within the database.

Impact:

WARNING: Failure to whitelist the correct networks will result in a connection loss.

WARNING: Changes to Cosmos DB firewalls may take up to 15 minutes to apply. Ensure that sufficient time is planned for remediation or changes to avoid disruption.

Audit:

From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade
3. Select a Cosmos DB to audit.
4. Select **Networking**.
5. Under **Public network access**, ensure **Selected networks** is selected.
6. Under **Virtual networks**, ensure appropriate virtual networks are configured.

From Azure CLI

Retrieve a list of all CosmosDB database names:

```
az cosmosdb list
```

For each database listed, run the following command:

```
az cosmosdb show <database id>
```

For each database, ensure that **isVirtualNetworkFilterEnabled** is set to **true**

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [862e97cf-49fc-4a5c-9de4-40d4e2e7c8eb](#) - **Name:** 'Azure Cosmos DB accounts should have firewall rules'

Remediation:

From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select a Cosmos DB account to audit.
4. Select **Networking**.
5. Under **Public network access**, select **Selected networks**.
6. Under **Virtual networks**, select **+ Add existing virtual network** or **+ Add a new virtual network**.
7. For existing networks, select subscription, virtual network, subnet and click **Add**. For new networks, provide a name, update the default values if required, and click **Create**.
8. Click **Save**.











Default Value:

By default, Cosmos DBs are set to have access all networks.

References:

1. <https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>
2. <https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-vnet-service-endpoint>
3. <https://docs.microsoft.com/en-us/cli/azure/cosmosdb?view=azure-cli-latest#az-cosmosdb-show>
4. <https://docs.microsoft.com/en-us/cli/azure/cosmosdb/database?view=azure-cli-latest#az-cosmosdb-database-list>
5. <https://docs.microsoft.com/en-us/powershell/module/az.cosmosdb/?view=azps-8.1.0>
6. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	14.1 <u>Segment the Network Based on Sensitivity</u> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).			

3.2 Ensure That Private Endpoints Are Used Where Possible (Automated)

Profile Applicability:

- Level 2

Description:

Private endpoints limit network traffic to approved sources.

Rationale:

For sensitive data, private endpoints allow granular control of which services can communicate with Cosmos DB and ensure that this network traffic is private. You set this up on a case by case basis for each service you wish to be connected.

Impact:

Only whitelisted services will have access to communicate with the Cosmos DB.

Audit:

From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select the Azure Cosmos DB account.
4. Select **Networking**.
5. Ensure **Public network access** is set to **Selected networks**.
6. Ensure the listed networks are set appropriately.
7. Select **Private access**.
8. Ensure a private endpoint exists and **Connection state** is **Approved**.

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [58440f8a-10c5-4151-bdce-dfbaad4a20b7](#) - **Name:** 'CosmosDB accounts should use private link'

Remediation:

From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select the Azure Cosmos DB account.
4. Select **Networking**.
5. Select **Private access**.
6. Click **+ Private Endpoint**.
7. Provide a Name.
8. Click **Next**.
9. From the Resource type drop down, select **Microsoft.AzureCosmosDB/databaseAccounts**.
10. From the Resource drop down, select the Cosmos DB account.
11. Click **Next**.
12. Provide appropriate Virtual Network details.
13. Click **Next**.
14. Provide appropriate DNS details.
15. Click **Next**.
16. Optionally provide Tags.
17. Click **Next : Review + create**.
18. Click **Create**.





Default Value:

By default Cosmos DB does not have private endpoints enabled and its traffic is public to the network.

References:

1. <https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>
2. <https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-cosmosdb-portal>
3. <https://docs.microsoft.com/en-us/cli/azure/cosmosdb/private-endpoint-connection?view=azure-cli-latest>
4. <https://docs.microsoft.com/en-us/cli/azure/network/private-endpoint?view=azure-cli-latest#az-network-private-endpoint-create>
5. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

CIS Controls:

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

3.3 Use Entra ID Client Authentication and Azure RBAC where possible. (Manual)

Profile Applicability:

- Level 1

Description:

Cosmos DB can use tokens or Entra ID for client authentication which in turn will use Azure RBAC for authorization. Using Entra ID is significantly more secure because Entra ID handles the credentials and allows for MFA and centralized management, and the Azure RBAC better integrated with the rest of Azure.

Rationale:

Entra ID client authentication is considerably more secure than token-based authentication because the tokens must be persistent at the client. Entra ID does not require this.

Audit:

From Powershell:

```
$cosmosdbname = "<your-cosmos-db-account-name>"
$resourcegroup = "<your-resource-group-name>"
az cosmosdb show --name $cosmosdbname --resource-group $resourcegroup |
ConvertFrom-Json
```

In the resulting output, `disableLocalAuth` should be true

Remediation:

Map all the resources that currently access to the Azure Cosmos DB account with keys or access tokens.

Create an Entra ID identity for each of these resources:

- For Azure resources, you can create a managed identity. You may choose between system-assigned and user-assigned managed identities.
- For non-Azure resources, create an Entra ID identity. Grant each Entra ID identity the minimum permission it requires. When possible, we recommend you use one of the 2 built-in role definitions: Cosmos DB Built-in Data Reader or Cosmos DB Built-in Data Contributor. Validate that the new resource is functioning correctly. After new permissions are granted to identities, it may take a few hours until they propagate. When all resources are working correctly with the new identities, continue to the next step.

From Powershell:

```
$cosmosdbname = "<your-cosmos-db-account-name>"
$resourcegroup = "<your-resource-group-name>"
az cosmosdb show --name $cosmosdbname --resource-group $resourcegroup |
ConvertFrom-Json
az resource update --ids $cosmosdb.id --set properties.disableLocalAuth=true
--latest-include-preview
```





Default Value:

The default is to use tokens/keys for client authentication.

References:

1. <https://learn.microsoft.com/en-us/azure/cosmos-db/role-based-access-control>

CIS Controls:

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

4 Azure Data Factory

Azure Product Page: <https://azure.microsoft.com/en-us/products/data-factory/>

Azure Policy for Data Factory: <https://learn.microsoft.com/en-us/azure/data-factory/policy-reference>

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

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

5 Azure Database for MariaDB (Retiring)

IMPORTANT NOTE: Azure Database for MariaDB will be retiring on **September 19, 2025**. If you are using Azure Database for MariaDB, you will need to migrate your workload to Azure Database for MySQL Flexible Server before **September 19, 2025**. Please review Microsoft's announcement on this service retirement here:

<https://azure.microsoft.com/en-us/updates/azure-database-for-mariadb-will-be-retired-on-19-september-2025-migrate-to-azure-database-for-mysql-flexible-server/>

Azure Product Page: <https://azure.microsoft.com/en-us/products/mariadb/>

6 Azure Database for MySQL

This section covers security best practice recommendations for Azure MySQL Database Servers.

Azure Product Page: <https://azure.microsoft.com/en-us/products/mysql/>

6.1 Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable **SSL connection** on **MYSQL** Servers.

Rationale:

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

Audit:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **Azure Database for MySQL servers**
3. For each database, click on **Connection security**
4. In **SSL** settings, ensure **Enforce SSL connection** is set to **ENABLED**.

From Azure CLI

Ensure the output of the below command returns ENABLED.

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

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [e802a67a-daf5-4436-9ea6-f6d821dd0c5d](#) - **Name:** 'Enforce SSL connection should be enabled for MySQL database servers'

Remediation:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **Azure Database for MySQL servers**
3. For each database, click on **Connection security**
4. In **SSL** settings, click on **ENABLED** to **Enforce SSL connections**

From Azure CLI

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

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

Default Value:

Azure Database for MySQL when provisioned through the Azure portal or CLI will require SSL connections by default.

References:

1. <https://docs.microsoft.com/en-us/azure/mysql/single-server/concepts-ssl-connection-security>
2. <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-ssl>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit>

CIS Controls:

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

6.2 Ensure 'TLS Version' is set to 'TLSV1.2' (or higher) for MySQL flexible Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Ensure **TLS version** on **MySQL flexible** servers is set to use TLS version 1.2 or higher.

Rationale:

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

Audit:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **Azure Database for MySQL flexible servers**
3. For each database, click on **Server parameters** under **Settings**
4. In the search box, type in **tls_version**
5. Ensure **tls_version** is set to **TLSV1.2** (or higher)

From Azure CLI

Ensure the output of the below command contains the key value pair "**values**": "**TLSV1.2**" (or higher).

```
az mysql flexible-server parameter show --name tls_version --resource-group <resourceGroupName> --server-name <serverName>
```

Example output (next page):

```
{
  "allowedValues": "TLSv1,TLSv1.1,TLSv1.2",
  "dataType": "Set",
  "defaultValue": "TLSv1.2",
  "description": "Which protocols the server permits for encrypted
connections. By default, TLS 1.2 is enforced",
  "id":
"/subscriptions/<subscriptionId>/resourceGroups/<resourceGroupName>/providers
/Microsoft.DBforMySQL/flexibleServers/<serverName>/configurations/tls_version
",
  "isConfigPendingRestart": "False",
  "isDynamicConfig": "False",
  "isReadOnly": "False",
  "name": "tls_version",
  "resourceGroup": "<resourceGroupName>",
  "source": "system-default",
  "systemData": null,
  "type": "Microsoft.DBforMySQL/flexibleServers/configurations",
  "value": "TLSv1.2"
}
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [49e6f04d-fbc3-4ac3-9e84-6ae0eb5db024](#) - **Name:** 'Require Secure Transport should be enabled for MySQL flexible servers'

Remediation:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to **Azure Database for MySQL flexible servers**
3. For each database, click on **Server parameters** under **Settings**
4. In the search box, type in **tls_version**
5. Click on the VALUE dropdown, and ensure only **TLSV1.2** (or higher) is selected for **tls_version**

From Azure CLI

Use the below command to set MYSQL flexible databases to used version 1.2 for the **tls_version** parameter.

```
az mysql flexible-server parameter set --name tls_version --resource-
group <resourceGroupName> --server-name <serverName> --value TLSV1.2
```





Default Value:

By default, TLS is set to v1.2 for MySQL Flexible servers.

References:

1. <https://docs.microsoft.com/en-us/azure/mysql/concepts-ssl-connection-security>
2. <https://docs.microsoft.com/en-us/azure/mysql/howto-configure-ssl>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default>

CIS Controls:

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

6.3 Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server (Manual)

Profile Applicability:

- Level 2

Description:

Enable audit_log_enabled on MySQL Servers.

Rationale:

Enabling audit_log_enabled helps MySQL Database to log items such as connection attempts to the server, DDL/DML access, and more. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Impact:

There are further costs incurred for storage of logs. For high traffic databases these logs will be significant. Determine your organization's needs before enabling.

Audit:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Select **Azure Database for MySQL Servers**
3. For each database, under the Settings section in the sidebar, select **Server parameters**
4. Ensure the **audit_log_enabled** parameter is set to **ON**

Remediation:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>.
2. Select **Azure Database for MySQL Servers**.
3. Select a database.
4. Under Settings, select **Server parameters**.
5. Update **audit_log_enabled** parameter to **ON**
6. Under Monitoring, select **Diagnostic settings**.
7. Select **+ Add diagnostic setting**.
8. Provide a diagnostic setting name.
9. Under Categories, select **MySQL Audit Logs**.
10. Specify destination details.
11. Click **Save**.

It may take up to 10 minutes for the logs to appear in the configured destination.

Default Value:

`audit_log_enabled` is set to **OFF** by default

References:







1. <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-portal>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

Additional Information:

There is also a CLI version: <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-cli>

There are numerous settings and event types and it might be helpful to discuss which of these may be appropriate to have a separate check item for.

CIS Controls:

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

6.4 Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server (Manual)

Profile Applicability:

- Level 2

Description:

Set `audit_log_enabled` to include CONNECTION on MySQL Servers.

Rationale:

Enabling CONNECTION helps MySQL Database to log items such as successful and failed connection attempts to the server. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Impact:

There are further costs incurred for storage of logs. For high traffic databases these logs will be significant. Determine your organization's needs before enabling.

Audit:

From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Azure Database for MySQL servers`.
3. Select a database.
4. Under `Settings`, select `Server parameters`.
5. Ensure `audit_log_enabled` parameter is set to `ON`.
6. Ensure `audit_log_events` parameter has `CONNECTION` checked.

Remediation:

From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Azure Database for MySQL servers`.
3. Select a database.
4. Under `Settings`, select `Server parameters`.
5. Update `audit_log_enabled` parameter to `ON`.
6. Update `audit_log_events` parameter to have at least `CONNECTION` checked.
7. Click `Save`.
8. Under `Monitoring`, select `Diagnostic settings`.
9. Select `+ Add diagnostic setting`.
10. Provide a diagnostic setting name.
11. Under `Categories`, select `MySQL Audit Logs`.

12. Specify destination details.
13. Click **Save**.

It may take up to 10 minutes for the logs to appear in the configured destination.

Default Value:

By default **audit_log_events** is disabled.







References:

1. <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-portal>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

Additional Information:

There is also a CLI version: <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-cli>

CIS Controls:

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

7 Azure Database for PostgreSQL

This section covers security best practice recommendations for Azure PostgreSQL Database Servers.

Azure Product Page: <https://azure.microsoft.com/en-us/products/postgresql/>

RETIREMENT of Azure PostgreSQL Single Server: Azure PostgreSQL Single Server is slated for retirement by March 25, 2025. Azure PostgreSQL Flexible Server is the newer deployment standard and is unaffected. Please use these resources to consider and prepare for migration:

- <https://learn.microsoft.com/en-us/azure/postgresql/single-server/whats-happening-to-postgresql-single-server>
- <https://learn.microsoft.com/en-us/azure/postgresql/migrate/concepts-single-to-flexible>

7.1 Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable **SSL connection** on **PostgreSQL** Servers.

Rationale:

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

Audit:

From Azure Portal

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

From Azure CLI

Ensure the output of the below command returns **Enabled**.

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

From PowerShell

Ensure the output of the below command returns **Enabled**.

```
Get-AzPostgreSqlServer -ResourceGroupName <ResourceGroupName> -ServerName  
<ServerName> | Select-Object SslEnforcement
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/%2FDefinitions

- **Policy ID:** [d158790f-bfb0-486c-8631-2dc6b4e8e6af](#) - **Name:** 'Enforce SSL connection should be enabled for PostgreSQL database servers'

Remediation:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for **PostgreSQL** server
3. For each database, click on **Connection security**
4. In **SSL** settings, click on **ENABLED** to enforce SSL connections
5. Click **Save**

From Azure CLI

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

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

From PowerShell

```
Update-AzPostgreSqlServer -ResourceGroupName <ResourceGroupName> -ServerName  
<ServerName> -SslEnforcement Enabled
```





Default Value:

By default, secure connectivity is enforced, but some application frameworks may not enable it during deployment.

References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-ssl-connection-security>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default>
3. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresserver?view=azps-9.2.0#example-2-get-postgresql-server-by-resource-group-and-server-name>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresserver?view=azps-9.2.0#example-1-update-postgresql-server-by-resource-group-and-server-name>

CIS Controls:

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

7.2 Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable **log_checkpoints** on PostgreSQL Servers.

Rationale:

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

Audit:

From Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to **Azure Database for PostgreSQL servers**.
3. For each database, click on **Server parameters**.
4. Search for **log_checkpoints**.
5. Ensure that value is set to **ON**.

From Azure CLI

Ensure value is set to **ON**

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

From PowerShell

Ensure value is set to **ON**

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -  
ServerName <ServerName> -Name log_checkpoints
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [eb6f77b9-bd53-4e35-a23d-7f65d5f0e43d](#) - **Name:** 'Log checkpoints should be enabled for PostgreSQL database servers'

Remediation:

From Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to **Azure Database for PostgreSQL servers**.
3. For each database, click on **Server parameters**.
4. Search for **log_checkpoints**.
5. Click **ON** and save.

From Azure CLI

Use the below command to update **log_checkpoints** configuration.

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

From PowerShell

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_checkpoints -Value on
```







Default Value:

By default **log_checkpoints** is enabled (set to **on**).

References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
4. <https://learn.microsoft.com/en-us/azure/postgresql/single-server/concepts-server-logs#configure-logging>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
6. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

CIS Controls:

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

7.3 Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable **log_connections** on PostgreSQL Servers.

Rationale:

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

Audit:

From Azure Portal

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

From Azure CLI

Ensure **log_connections** value is set to **ON**

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

From PowerShell

Ensure **log_connections** value is set to **ON**

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_connections
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [eb6f77b9-bd53-4e35-a23d-7f65d5f0e442](#) - **Name:** 'Log connections should be enabled for PostgreSQL database servers'

Remediation:

From Azure Portal

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

From Azure CLI

Use the below command to update **log_connections** configuration.

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

From PowerShell

Use the below command to update **log_connections** configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_connections -Value on
```




Default Value:




By default **log_connections** is enabled (set to **on**).

References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

7.4 Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable **log_disconnections** on **PostgreSQL Servers**.

Rationale:

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

Impact:

Enabling this setting will enable a log of all disconnections. If this is enabled for a high traffic server, the log may grow exponentially.

Audit:

From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to **Azure Database for PostgreSQL servers**
3. For each database, click on **Server parameters**
4. Search for **log_disconnections**.
5. Ensure that value is set to **ON**.

From Azure CLI

Ensure **log_disconnections** value is set to **ON**

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

From PowerShell

Ensure **log_disconnections** value is set to **ON**

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_disconnections
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [eb6f77b9-bd53-4e35-a23d-7f65d5f0e446](#) - **Name:** 'Disconnections should be logged for PostgreSQL database servers.'

Remediation:

From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to **Azure Database** for **PostgreSQL servers**
3. For each database, click on **Server parameters**
4. Search for **log_disconnections**.
5. Click **ON** and save.

From Azure CLI

Use the below command to update **log_disconnections** configuration.

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

From PowerShell

Use the below command to update **log_disconnections** configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_disconnections -Value on
```







Default Value:

By default **log_disconnections** is disabled (set to **off**).

References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

CIS Controls:

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

7.5 Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable **connection_throttling** on **PostgreSQL Servers**.

Rationale:

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

Audit:

From Azure Portal

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

From Azure CLI

Ensure **connection_throttling** value is set to **ON**

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

From PowerShell

Ensure **connection_throttling** value is set to **ON**

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name connection_throttling
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [5345bb39-67dc-4960-a1bf-427e16b9a0bd](#) - **Name:** 'Connection throttling should be enabled for PostgreSQL database servers'

Remediation:

From Azure Portal

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

From Azure CLI

Use the below command to update **connection_throttling** configuration.

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

From PowerShell

Use the below command to update **connection_throttling** configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name connection_throttling -Value on
```




Default Value:




By default, **connection_throttling** is enabled (set to **on**).

References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

7.6 Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Ensure `log_retention_days` on `PostgreSQL Servers` is set to an appropriate value.

Rationale:

Configuring `log_retention_days` determines the duration in days that `Azure Database for PostgreSQL` retains log files. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Impact:

Configuring this setting will result in logs being retained for the specified number of days. If this is configured on a high traffic server, the log may grow quickly to occupy a large amount of disk space. In this case you may want to set this to a lower number.

Audit:

From Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Azure Database for PostgreSQL servers`.
3. For each database, click on `Server parameters`.
4. Search for `log_retention_days`.
5. Ensure that the `value` is between 4 and 7 (inclusive).

From Azure CLI

Ensure `log_retention_days` value is greater than 3.

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

From Powershell

Ensure `log_retention_days` value is greater than 3.

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -  
ServerName <ServerName> -Name log_retention_days
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [eb6f77b9-bd53-4e35-a23d-7f65d5f0e8f3](#) - **Name:** 'Log duration should be enabled for PostgreSQL database servers'
- **Policy ID:** [5e1de0e3-42cb-4ebc-a86d-61d0c619ca48](#) - **Name:** 'Public network access should be disabled for PostgreSQL flexible servers'

Remediation:

From Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to **Azure Database for PostgreSQL servers**.
3. For each database, click on **Server parameters**.
4. Search for **log_retention_days**.
5. Input a value between 4 and 7 (inclusive) and click **Save**.

From Azure CLI

Use the below command to update **log_retention_days** configuration.

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

From Powershell

Use the below command to update **log_retention_days** configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_retention_days -Value <4-7>
```

Default Value:






By default **log_retention_days** is set to **3**.

References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
2. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-6-configure-log-storage-retention>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>

5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

7.7 Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Automated)

Profile Applicability:

- Level 1

Description:

Disable access from Azure services to PostgreSQL Database Server.

Rationale:

If access from Azure services is enabled, the server's firewall will accept connections from all Azure resources, including resources not in your subscription. This is usually not a desired configuration. Instead, set up firewall rules to allow access from specific network ranges or VNET rules to allow access from specific virtual networks.

Audit:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>.
2. Go to **Azure Database for PostgreSQL servers**.
3. For each database, click on **Connection security**.
4. Under **Firewall rules**, ensure **Allow access to Azure services** is set to **No**.

From Azure CLI

Ensure the output of the below command does not include a rule with the name **AllowAllWindowsAzureIps** or "startIpAddress": "0.0.0.0" or "endIpAddress": "0.0.0.0",

```
az postgres server firewall-rule list --resource-group <resourceGroupName> -  
-server <serverName>
```

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [b52376f7-9612-48a1-81cd-1ffe4b61032c](#) - **Name:** 'Public network access should be disabled for PostgreSQL servers'
- **Policy ID:** [5e1de0e3-42cb-4ebc-a86d-61d0c619ca48](#) - **Name:** 'Public network access should be disabled for PostgreSQL flexible servers'

Remediation:

From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>.
2. Go to **Azure Database for PostgreSQL servers**.
3. For each database, click on **Connection security**.
4. Under **Firewall rules**, set **Allow access to Azure services** to **No**.
5. Click **Save**.

From Azure CLI

Use the below command to delete the AllowAllWindowsAzureIps rule for PostgreSQL Database.

```
az postgres server firewall-rule delete --name AllowAllWindowsAzureIps --resource-group <resourceGroupName> --server-name <serverName>
```







Default Value:

The Azure Postgres firewall is set to block all access by default.

References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-firewall-rules>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-manage-firewall-using-cli>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries>
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-6-deploy-web-application-firewall>

CIS Controls:

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

7.8 Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Single Server Only) (Automated)

Profile Applicability:

- Level 1

Description:

Azure Database for PostgreSQL servers should be created with 'infrastructure double encryption' enabled.

NOTE: This recommendation currently only applies to Single Server, not Flexible Server. See additional information below for details about the planned retirement of Azure PostgreSQL Single Server.

Rationale:

If Double Encryption is enabled, another layer of encryption is implemented at the hardware level before the storage or network level. Information will be encrypted before it is even accessed, preventing both interception of data in motion if the network layer encryption is broken and data at rest in system resources such as memory or processor cache. Encryption will also be in place for any backups taken of the database, so the key will secure access the data in all forms. For the most secure implementation of key based encryption, it is recommended to use a Customer Managed asymmetric RSA 2048 Key in Azure Key Vault.

Impact:

The read and write speeds to the database will be impacted if both default encryption and Infrastructure Encryption are checked, as a secondary form of encryption requires more resource overhead for the cryptography of information. This cost is justified for information security. Customer managed keys are recommended for the most secure implementation, leading to overhead of key management. The key will also need to be backed up in a secure location, as loss of the key will mean loss of the information in the database.

Audit:

From Azure Portal

1. From Azure Home, click on more services.
2. Click on Databases.
3. Click on Azure Database for PostgreSQL servers.
4. Select the database by clicking on its name.
5. Under Security, click Data encryption.
6. Ensure that 'Infrastructure encryption enabled' is displayed and is 'checked'.

From Azure CLI

1. Enter the command

```
az postgres server configuration show --name <servername> --resource-group <resourcegroup> --query 'properties.infrastructureEncryption' -o tsv
```

2. Verify that Infrastructure encryption is enabled.

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [24fba194-95d6-48c0-aea7-f65bf859c598](#) - **Name:** 'Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers'

Remediation:

It is not possible to enable 'infrastructure double encryption' on an existing Azure Database for PostgreSQL server.

The remediation steps detail the creation of a new Azure Database for PostgreSQL server with 'infrastructure double encryption' enabled.

From Azure Portal

1. Go through the normal process of database creation.
2. On step 2 titled 'Additional settings' ensure that 'Infrastructure double encryption enabled' is 'checked'.
3. Acknowledge that you understand this will impact database performance.
4. Finish database creation as normal.

From Azure CLI

```
az postgres server create --resource-group <resourcegroup> --name <servername> --location <location> --admin-user <adminusername> --admin-password <server_admin_password> --sku-name GP_Gen4_2 --version 11 --infrastructure-encryption Enabled
```

Default Value:

By Default, Double Encryption is disabled.

References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/howto-double-encryption>
2. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-infrastructure-double-encryption>
3. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-data-encryption-postgresql>
4. <https://docs.microsoft.com/en-us/azure/key-vault/keys/byok-specification>
5. <https://docs.microsoft.com/en-us/azure/postgresql/howto-double-encryption>
6. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default>

Additional Information:

RETIREMENT of Azure PostgreSQL Single Server: Azure PostgreSQL Single Server is slated for retirement by March 25, 2025. Please use these resources to consider and prepare for migration:

- <https://learn.microsoft.com/en-us/azure/postgresql/single-server/whats-happening-to-postgresql-single-server>
- <https://learn.microsoft.com/en-us/azure/postgresql/migrate/concepts-single-to-flexible>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

8 Azure Database Migration Service

Azure Product Page: <https://azure.microsoft.com/en-us/products/database-migration/>

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

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

9 Azure SQL (Reference)

Azure SQL is a family of Azure products for the Microsoft SQL Server database engine. For security best practice recommendations for this family of products, please use the brief descriptions below to reference the appropriate section of this Benchmark for the Azure SQL sub-product which is relevant to your environment:

- **Azure SQL Database - "SQL DB" - (Section 10):** A managed Platform as a Service (PaaS) implementation of SQL with a smaller set of the features than Azure SQL MI*.
- **Azure SQL Edge (Section 11):** A relational database engine optimized for Internet of Things (IoT) and edge compute applications and solutions.
- **Azure SQL Managed Instance - "SQL MI" - (Section 12):** A managed Platform as a Service (PaaS) implementation of SQL with a larger set of features than Azure SQL DB*.
- **SQL Server on Azure Virtual Machines (Section 13):** An implementation of SQL Server that relies on the use of a dedicated virtual machine.

*To better understand the feature differences between Azure SQL Database (SQL DB) and Azure SQL Managed Instance (SQL MI), please refer to this document:

<https://learn.microsoft.com/en-us/azure/azure-sql/database/features-comparison?view=azuresql>

Azure Product Page: <https://azure.microsoft.com/en-us/products/azure-sql/>

10 Azure SQL Database

This section covers security best practice recommendations for Azure SQL Database.

Azure Product Page: <https://azure.microsoft.com/en-us/products/azure-sql/database/>

10.1 Ensure that 'Auditing' is set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

Enable auditing on SQL Servers.

Rationale:

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

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

Audit:

From Azure Portal

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

From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerAudit -ResourceGroupName <ResourceGroupName> -ServerName  
<SQLServerName>
```

Ensure that **BlobStorageTargetState**, **EventHubTargetState**, or **LogAnalyticsTargetState** is set to **Enabled**.

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~Definitions

- **Policy ID:** [a6fb4358-5bf4-4ad7-ba82-2cd2f41ce5e9](#) - **Name:** 'Auditing on SQL server should be enabled'

Remediation:

From Azure Portal

1. Go to **SQL servers**
2. Select the SQL server instance
3. Under **Security**, click **Auditing**
4. Click the toggle next to **Enable Azure SQL Auditing**
5. Select an Audit log destination
6. Click **Save**

From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server, enable auditing and set the retention for at least 90 days.

Log Analytics Example

```
Set-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName  
<SQL Server name> -RetentionInDays <Number of Days to retain the audit logs,  
should be 90days minimum> -LogAnalyticsTargetState Enabled -  
WorkspaceResourceId "/subscriptions/<subscription  
ID>/resourceGroups/insights-  
integration/providers/Microsoft.OperationalInsights/workspaces/<workspace  
name>
```

Event Hub Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName  
"<SQL Server name>" -EventHubTargetState Enabled -EventHubName  
"<Event Hub name>" -EventHubAuthorizationRuleResourceId "<Event Hub  
Authorization Rule Resource ID>"
```

Blob Storage Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -BlobStorageTargetState Enabled
    -StorageAccountResourceId
"/subscriptions/<subscription_ID>/resourceGroups/<Resource_Group>/providers/M
icrosoft.Stora
ge/storageAccounts/<Storage Account name>"
```

Default Value:

By default, **Enable Azure SQL 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-azurermssqlserverauditing?view=azurermips-5.2.0>
3. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermssqlserverauditingpolicy?view=azurermips-5.2.0>
4. <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing>
5. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

Additional Information:

- A server policy applies to all existing and newly created databases on the server.
- If server blob auditing is enabled, it always applies to the database. The database will be audited, regardless of the database auditing settings. Auditing type table is already deprecated leaving only type blob available.
- Enabling blob auditing on the database, in addition to enabling it on the server, does not override or change any of the settings of the server blob auditing. Both audits will exist side by side. In other words, the database is audited twice in parallel; once by the server policy and once by the database policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

10.2 Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that no SQL Databases allow ingress from 0.0.0.0/0 (ANY IP).

Rationale:

Azure SQL Server includes a firewall to block access to unauthorized connections. More granular IP addresses can be defined by referencing the range of addresses available from specific datacenters.

By default, for a SQL server, a Firewall exists with StartIP of 0.0.0.0 and EndIP of 0.0.0.0 allowing access to all the Azure services.

Additionally, a custom rule can be set up with StartIP of 0.0.0.0 and EndIP of 255.255.255.255 allowing access from ANY IP over the Internet.

In order to reduce the potential attack surface for a SQL server, firewall rules should be defined with more granular IP addresses by referencing the range of addresses available from specific datacenters.

Impact:

Disabling **Allow Azure services and resources to access this server** will break all connections to SQL server and Hosted Databases unless custom IP specific rules are added in Firewall Policy.

Audit:

From Azure Portal

1. Go to **SQL servers**
2. For each SQL server
3. Click on **Networking**
4. Ensure that **Allow Azure services and resources to access this server** is **Unchecked**
5. Ensure that no firewall rule exists with
 - Start IP of **0.0.0.0**
 - or other combinations which allows access to wider public IP ranges

From Azure CLI

List all SQL servers

```
az sql server list
```

For each SQL server run the following command

```
az sql server firewall-rule list --resource-group <resource group name> --server <sql server name>
```

Ensure the output does not contain any firewall **allow** rules with a source of **0.0.0.0**, or any rules named **AllowAllWindowsAzureIps**

From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

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

Ensure that **StartIpAddress** is not set to **0.0.0.0**, **/0** or other combinations which allows access to wider public IP ranges including Windows Azure IP ranges. Also ensure that **FirewallRuleName** doesn't contain **AllowAllWindowsAzureIps** which is the rule created when the **Allow Azure services and resources to access this server** setting is enabled for that SQL Server.

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [1b8ca024-1d5c-4dec-8995-b1a932b41780](#) - **Name:** 'Public network access on Azure SQL Database should be disabled'

Remediation:

From Azure Portal

1. Go to **SQL servers**
2. For each SQL server
3. Click on **Networking**
4. **Uncheck** the checkbox for **Allow Azure services and resources to access this server**
5. Set firewall rules to limit access to only authorized connections

From Azure CLI

Disable default firewall rule **Allow access to Azure services**:

```
az sql server firewall-rule delete --resource-group <resource group> --server <sql server name> --name "AllowAllWindowsAzureIps"
```

Remove a custom firewall rule:

```
az sql server firewall-rule delete --resource-group <resource group> --server <sql server name> --name <firewall rule name>
```

Create a firewall rule:

```
az sql server firewall-rule create --resource-group <resource group> --server <sql server name> --name <firewall rule name> --start-ip-address "<IP Address other than 0.0.0.0>" --end-ip-address "<IP Address other than 0.0.0.0 or 255.255.255.255>"
```

Update a firewall rule:

```
az sql server firewall-rule update --resource-group <resource group> --server <sql server name> --name <firewall rule name> --start-ip-address "<IP Address other than 0.0.0.0>" --end-ip-address "<IP Address other than 0.0.0.0 or 255.255.255.255>"
```

From PowerShell

Disable Default Firewall Rule **Allow access to Azure services** :

```
Remove-AzSqlServerFirewallRule -FirewallRuleName "AllowAllWindowsAzureIps" -ResourceGroupName <resource group name> -ServerName <server name>
```

Remove a custom Firewall rule:

```
Remove-AzSqlServerFirewallRule -FirewallRuleName "<firewall rule name>" -ResourceGroupName <resource group name> -ServerName <server name>
```

Set the appropriate firewall rules:

```
Set-AzSqlServerFirewallRule -ResourceGroupName <resource group name> -ServerName <server name> -FirewallRuleName "<firewall rule name>" -StartIpAddress "<IP Address other than 0.0.0.0>" -EndIpAddress "<IP Address other than 0.0.0.0 or 255.255.255.255>"
```

Default Value:

By default, **Allow access to Azure Services** is set to **NO**.

References:







1. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-windows-firewall-for-database-engine-access?view=sql-server-2017>
2. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermssqlserverfirewallrule?view=azurermps-5.2.0>

3. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermssqlserverfirewallrule?view=azurermmps-5.2.0>
4. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/remove-azurermssqlserverfirewallrule?view=azurermmps-5.2.0>
5. <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure>
6. <https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-set-database-firewall-rule-azure-sql-database?view=azuresqldb-current>
7. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls>

Additional Information:

Firewall rules configured on individual SQL Database using Transact-sql overrides the rules set on SQL server. Azure does not provide any Powershell, API, CLI, Portal option to check database level firewall rules, and so far Transact-SQL is the only way to check for the same. For comprehensive control over egress traffic on SQL Databases, Firewall rules should be checked using SQL client.

CIS Controls:

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

10.3 Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated)

Profile Applicability:

- Level 2

Description:

Transparent Data Encryption (TDE) with Customer-managed key support provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties.

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

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

Rationale:

Customer-managed key support for Transparent Data Encryption (TDE) allows user control of TDE encryption keys and restricts who can access them and when. Azure Key Vault, Azure's cloud-based external key management system, is the first key management service where TDE has integrated support for Customer-managed keys. With Customer-managed key support, the database encryption key is protected by an asymmetric key stored in the Key Vault. The asymmetric key is set at the server level and inherited by all databases under that server.

Impact:

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

When deploying Customer Managed Keys, it is prudent to ensure that you also deploy an automated toolset for managing these keys (this should include discovery and key rotation), and Keys should be stored in an HSM or hardware backed keystore, such as Azure Key Vault.

As far as toolsets go, check with your cryptographic key provider, as they may well provide one as an add-on to their service.

Audit:

From Azure Portal

1. Go to **SQL servers**

For the desired server instance

2. Click On **Transparent data encryption**
3. Ensure that **Customer-managed key** is selected
4. Ensure **Make selected key the default TDE protector** is checked

From Azure CLI

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

Ensure the output of the command contains properties

kind set to **azurekeyvault**

serverKeyType set to **AzureKeyVault**

uri is not null

From PowerShell

```
Get-AzSqlServerTransparentDataEncryptionProtector -ServerName <ServerName> -  
ResourceGroupName <ResourceGroupName>
```

Ensure the output of the command contains properties

Type set to **AzureKeyVault**

ServerKeyVaultKeyName set to **KeyVaultName_KeyName_KeyIdentifierVersion**

KeyId set to **KeyIdentifier**

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [0a370ff3-6cab-4e85-8995-295fd854c5b8](#) - **Name:** 'SQL servers should use customer-managed keys to encrypt data at rest'

- **Policy ID:** [ac01ad65-10e5-46df-bdd9-6b0cad13e1d2](#) - **Name:** 'SQL managed instances should use customer-managed keys to encrypt data at rest'

Remediation:

From Azure Console

1. Go to **SQL servers**

For the desired server instance

2. Click On **Transparent data encryption**
3. Set **Transparent data encryption** to **Customer-managed key**
4. Browse through your **key vaults** to Select an existing key or create a new key in the Azure Key Vault.
5. Check **Make selected key the default TDE protector**

From Azure CLI

Use the below command to encrypt SQL server's TDE protector with a Customer-managed key

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

From PowerShell

Use the below command to encrypt SQL server's TDE protector with a Customer-managed Key Vault key

```
Set-AzSqlServerTransparentDataEncryptionProtector -Type AzureKeyVault -KeyId <KeyIdentifier> -ServerName <ServerName> -ResourceGroupName <ResourceGroupName>
```

Select **Y** when prompted

Default Value:

By Default, Microsoft managed TDE protector is enabled for a SQL server.

References:





1. <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-byok-azure-sql>
2. <https://azure.microsoft.com/en-in/blog/preview-sql-transparent-data-encryption-tde-with-bring-your-own-key-support/>
3. <https://winterdom.com/2017/09/07/azure-sql-tde-protector-keyvault>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>
5. <https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts>

6. <https://docs.microsoft.com/en-us/cli/azure/sql/server/tde-key?view=azure-cli-latest>
7. <https://learn.microsoft.com/en-us/powershell/module/az.sql/get-azsqlservertransparentdataencryptionprotector?view=azps-9.2.0>
8. <https://learn.microsoft.com/en-us/powershell/module/az.sql/set-azsqlservertransparentdataencryptionprotector?view=azps-9.2.0>

Additional Information:

- This configuration is audited or can be done only on SQL server. The same configuration will be in effect on SQL Databases hosted on SQL Server.
- Ensuring TDE is protected by a Customer-managed key on SQL Server does not ensure the encryption of SQL Databases. **Transparent Data Encryption : Data Encryption (ON/OFF)** setting on individual SQL Database decides whether database is encrypted or not.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

10.4 Ensure that Microsoft Entra authentication is Configured for SQL Servers (Automated)

Profile Applicability:

- Level 1

Description:

Use Microsoft Entra authentication for authentication with SQL Database to manage credentials in a single place.

Rationale:

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

- It provides an alternative to SQL Server authentication.
- Helps stop the proliferation of user identities across database servers.
- Allows password rotation in a single place.
- Customers can manage database permissions using external (Entra ID) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Microsoft Entra.
- Entra ID authentication uses contained database users to authenticate identities at the database level.
- Entra ID supports token-based authentication for applications connecting to SQL Database.
- Entra ID authentication supports ADFS (domain federation) or native user/password authentication for a local Active Directory without domain synchronization.
- Entra ID 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.

Impact:

This will create administrative overhead with user account and permission management. For further security on these administrative accounts, you may want to consider licensing which supports features like Multi Factor Authentication.

Audit:

From Azure Portal

1. Go to **SQL servers**
2. For each SQL server, click on **Microsoft Entra admin** under the Settings section
3. Ensure that a value has been set for **Admin Name** under the **Microsoft Entra admin** section

From Azure CLI

To list SQL Server Admins on a specific server:

```
az sql server ad-admin list --resource-group <resource-group> --server <server>
```

From PowerShell

Print a list of all SQL Servers to find which one you want to audit

```
Get-AzSqlServer
```

Audit a list of Administrators on a Specific Server

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

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

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [1f314764-cb73-4fc9-b863-8eca98ac36e9](#) - **Name:** 'An Azure Active Directory administrator should be provisioned for SQL servers'

Remediation:

From Azure Portal

1. Go to **SQL servers**
2. For each SQL server, click on **Microsoft Entra admin**
3. Click on **Set admin**
4. Select an admin
5. Click **Save**

From Azure CLI

```
az ad user show --id
```

For each Server, set AD Admin

```
az sql server ad-admin create --resource-group <resource group name> --server  
<server name> --display-name <display name> --object-id <object id of user>
```

From PowerShell

For each Server, set Entra ID Admin

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

Default Value:

Entra ID Authentication for SQL Database/Server is not enabled by default





References:

1. <https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-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-azurermssqlserveractivedirectoryadministrator?view=azurerm-5.2.0>
4. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-1-use-centralized-identity-and-authentication-system>
5. https://docs.microsoft.com/en-us/cli/azure/sql/server/ad-admin?view=azure-cli-latest#az_sql_server_ad_admin_list

Additional Information:

NOTE - Assigning an Administrator in Entra ID is just the first step. When using Entra ID for central authentication there are many other groups and roles that need to be configured based on the needs of your organization. The How-to Guides should be used to determine what roles should be assigned and what groups should be created to manage permissions and access to resources.

CIS Controls:

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

10.5 Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)

Profile Applicability:

- Level 1

Description:

Enable Transparent Data Encryption on every SQL server.

Rationale:

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

Audit:

From Azure Portal

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**

From Azure CLI

Ensure the output of the below command is **Enabled**

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

From PowerShell

Get a list of SQL Servers.

```
Get-AzSqlServer
```

For each server, list the databases.

```
Get-AzSqlDatabase -ServerName <SQL Server Name> -ResourceGroupName <Resource  
Group Name>
```

For each database not listed as a **Master** database, check for Transparent Data Encryption.

```
Get-AzSqlDatabaseTransparentDataEncryption -ResourceGroupName <Resource Group Name> -ServerName <SQL Server Name> -DatabaseName <Database Name>
```

Make sure **DataEncryption** is **Enabled** for each database except the **Master** database.

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [17k78e20-9358-41c9-923c-fb736d382a12](#) - **Name:** 'Transparent Data Encryption on SQL databases should be enabled'

Remediation:

From Azure Portal

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

From Azure CLI

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
```

From PowerShell

Use the below command to enable **Transparent data encryption** for SQL DB instance.

```
Set-AzSqlDatabaseTransparentDataEncryption -ResourceGroupName <Resource Group Name> -ServerName <SQL Server Name> -DatabaseName <Database Name> -State 'Enabled'
```

Note:

- TDE cannot be used to encrypt the logical master database in SQL Database. The master database contains objects that are needed to perform the TDE operations on the user databases.
- Azure Portal does not show master databases per SQL server. However, CLI/API responses will show master databases.

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>
2. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default>
3. <https://learn.microsoft.com/en-us/powershell/module/az.sql/set-azsqldatabasetransparentdataencryption?view=azps-9.2.0>

Additional Information:

- Transparent Data Encryption (TDE) can be enabled or disabled on individual **SQL Database** level and not on the **SQL Server** level.
- TDE cannot be used to encrypt the logical master database in SQL Database. The master database contains objects that are needed to perform the TDE operations on the user databases.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	14.8 <u>Encrypt Sensitive Information at Rest</u> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

10.6 Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)

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:

From Azure Portal

1. Go to **SQL servers**
2. For each server instance
3. Click on **Auditing**
4. If storage is selected, expand **Advanced properties**
5. Ensure **Retention (days)** setting is greater than **90** days or **0** for unlimited retention.

From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

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

Ensure that **RetentionInDays** is set to **more than 90**

Note: If the SQL server is set with **LogAnalyticsTargetState** setting set to **Enabled**, run the following additional command.

```
Get-AzOperationalInsightsWorkspace | Where-Object {$_.ResourceId -eq <SQL  
Server WorkspaceResourceId>}
```

Ensure that **RetentionInDays** is set to **more than 90**

From Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~./Definitions

- **Policy ID:** [89099bee-89e0-4b26-a5f4-165451757743](#) - **Name:** 'SQL servers with auditing to storage account destination should be configured with 90 days retention or higher'

Remediation:

From Azure Portal

1. Go to **SQL servers**
2. For each server instance
3. Click on **Auditing**
4. If storage is selected, expand **Advanced properties**
5. Set the **Retention (days)** setting greater than **90** days or **0** for unlimited retention.
6. Select **Save**

From PowerShell

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

Log Analytics Example

```
Set-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName  
<SQL Server name> -RetentionInDays <Number of Days to retain the audit logs,  
should be more than 90 days> -LogAnalyticsTargetState Enabled -  
WorkspaceResourceId "/subscriptions/<subscription  
ID>/resourceGroups/insights-  
integration/providers/Microsoft.OperationalInsights/workspaces/<workspace  
name>
```

Event Hub Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName  
"<SQL Server name>" -EventHubTargetState Enabled -EventHubName  
"<Event Hub name>" -EventHubAuthorizationRuleResourceId "<Event Hub  
Authorization Rule Resource ID>"
```

Blob Storage Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -BlobStorageTargetState Enabled
    -StorageAccountResourceId
"/subscriptions/<subscription_ID>/resourceGroups/<Resource_Group>/providers/M
icrosoft.Stora
ge/storageAccounts/<Storage Account name>"
```






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-azurermsssqlserverauditing?view=azurerm-5.2.0>
3. <https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-6-configure-log-storage-retention>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

10.7 Ensure Public Network Access is Disabled (Manual)

Profile Applicability:

- Level 1

Description:

Disabling public network access restricts the service from accessing public networks.

Rationale:

A secure network architecture requires carefully constructed network segmentation. Public Network Access tends to be overly permissive and introduces unintended vectors for threat activity.

Impact:

Some architectural consideration may be necessary to ensure that required network connectivity is still made available. No additional cost or performance impact is required to deploy this recommendation.

Audit:

From Azure Portal

1. Search for and open the **SQL Server** service
2. For each SQL Server listed, repeat the remaining steps
3. Click on the name of the SQL Server
4. In the blade menu on the left, expand the **Security** section
5. Under the expanded Security section, click on **Networking**
6. Review the **Public access** tab in the networking window.

If the radio button under **Public network access** setting is set to **Disable**, the configuration for that SQL Server is compliant.

Remediation:

From Azure Portal

1. Search for and open the **SQL Server** service
2. For each SQL Server listed, repeat the remaining steps
3. Click on the name of the SQL Server
4. In the blade menu on the left, expand the **Security** section
5. Under the expanded Security section, click on **Networking**
6. Under the **Public access** tab in the networking window, set the **Public network access** setting to **Disable**.







Default Value:

By default, Azure SQL Server's Public network access is set to **Disable**.

References:

1. <https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>
2. <https://learn.microsoft.com/en-us/azure/azure-sql/database/connectivity-settings?view=azuresql&tabs=azure-portal#deny-public-network-access>

CIS Controls:

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

11 Azure SQL Edge

Azure Product Page: <https://azure.microsoft.com/en-us/products/azure-sql/edge/>

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

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

12 Azure SQL Managed Instance

This section covers security best practice recommendations for Azure SQL Managed Instance.

Azure Product Page: <https://azure.microsoft.com/en-us/products/azure-sql/managed-instance/>

No specific prescriptive guidance exists yet for Azure SQL Managed Instance. If you would like to contribute security best practice guidance for Azure SQL Managed Instance, please join the CIS Microsoft Azure Community at <https://workbench.cisecurity.org>.

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

13 SQL Server on Azure Virtual Machines

This section covers security best practice recommendations for SQL Server on Azure Virtual Machines.

Azure Product Page: <https://azure.microsoft.com/en-us/products/virtual-machines/sql-server/>

No specific prescriptive guidance exists yet for SQL Server on Azure Virtual Machines. If you would like to contribute security best practice guidance for SQL Server on Azure Virtual Machines, please join the CIS Microsoft Azure Community at <https://workbench.cisecurity.org>.

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

14 Table Storage (Reference)

Azure Product Page: <https://azure.microsoft.com/en-us/products/storage/tables/>

Table Storage in Azure is a sub-service of an Azure Storage Account. Security Best Practice recommendations improving the security of Table Storage are applied to the Azure Storage Account that is hosting the Table Storage, not configurable within the Table Storage sub-service. These recommendations will therefore be maintained in the "Storage Account" section of the CIS Microsoft Azure Storage Services Benchmark.

Microsoft Cloud Security Baseline for Storage Accounts: <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline?toc=%2Fazure%2Fstorage%2Ftables%2Ftoc.json%3Ftoc%3D%2Fazure%2Fstorage%2Ftables%2FTOC.json>

15 Azure Managed Instance for Apache Cassandra

Azure Product Page: <https://azure.microsoft.com/en-us/products/managed-instance-apache-cassandra/>

No prescriptive guidance exists yet for Azure Managed Instance for Apache Cassandra. If you would like to contribute security best practice guidance for Azure Managed Instance for Apache Cassandra, please join the CIS Microsoft Azure Community at <https://workbench.cisecurity.org>.

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

16 Azure confidential ledger

Azure Product Page: <https://azure.microsoft.com/en-us/products/azure-confidential-ledger/>

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

While this Service is under community development, we strongly recommend reviewing the relevant descriptive guidance provided by the Microsoft Cloud Security Benchmark here: <https://learn.microsoft.com/en-us/security/benchmark/azure/>

Please note that while Benchmark prescriptive guidance does not yet exist for this service, there are likely considerations for secure configuration that may require your due care and due diligence. To determine which aspects of configuration are the responsibility of the customer, and which are assumed by Microsoft, we recommend reviewing Microsoft's Shared Responsibility Model: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Introduction		
1.1	Multiple Methods of Audit and Remediation		
2	Azure Cache for Redis		
2.1	Ensure 'Microsoft Entra Authentication' is 'Enabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure that 'Allow access only via SSL' is set to 'Yes' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure that 'Minimum TLS version' is set to TLS v1.2 (or higher) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure that 'Access Policies' are implemented and reviewed periodically (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure that 'System Assigned Managed Identity' is set to 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure that 'Public Network Access' is 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3	Azure Cosmos DB		
3.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure That Private Endpoints Are Used Where Possible (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Use Entra ID Client Authentication and Azure RBAC where possible. (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4	Azure Data Factory		
5	Azure Database for MariaDB (Retiring)		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6	Azure Database for MySQL		
6.1	Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Ensure 'TLS Version' is set to 'TLSV1.2' (or higher) for MySQL flexible Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7	Azure Database for PostgreSQL		
7.1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.6	Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.8	Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Single Server Only) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8	Azure Database Migration Service		
9	Azure SQL (Reference)		
10	Azure SQL Database		
10.1	Ensure that 'Auditing' is set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
10.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
10.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
10.7	Ensure Public Network Access is Disabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
11	Azure SQL Edge		
12	Azure SQL Managed Instance		
13	SQL Server on Azure Virtual Machines		
14	Table Storage (Reference)		
15	Azure Managed Instance for Apache Cassandra		
16	Azure confidential ledger		

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure that 'Public Network Access' is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	<input type="checkbox"/>	<input type="checkbox"/>
10.7	Ensure Public Network Access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure 'Microsoft Entra Authentication' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure that 'Allow access only via SSL' is set to 'Yes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure that 'Minimum TLS version' is set to TLS v1.2 (or higher)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure that 'Public Network Access' is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure That Private Endpoints Are Used Where Possible	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Use Entra ID Client Authentication and Azure RBAC where possible.	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Ensure 'TLS Version' is set to 'TLSV1.2' (or higher) for MySQL flexible Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.6	Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	<input type="checkbox"/>	<input type="checkbox"/>
10.1	Ensure that 'Auditing' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	<input type="checkbox"/>	<input type="checkbox"/>
10.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	<input type="checkbox"/>	<input type="checkbox"/>
10.7	Ensure Public Network Access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure 'Microsoft Entra Authentication' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure that 'Allow access only via SSL' is set to 'Yes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure that 'Minimum TLS version' is set to TLS v1.2 (or higher)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure that 'Access Policies' are implemented and reviewed periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure that 'Public Network Access' is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure That Private Endpoints Are Used Where Possible	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Use Entra ID Client Authentication and Azure RBAC where possible.	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Ensure 'TLS Version' is set to 'TLSV1.2' (or higher) for MySQL flexible Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.6	Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	<input type="checkbox"/>	<input type="checkbox"/>
7.8	Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Single Server Only)	<input type="checkbox"/>	<input type="checkbox"/>
10.1	Ensure that 'Auditing' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	<input type="checkbox"/>	<input type="checkbox"/>
10.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	<input type="checkbox"/>	<input type="checkbox"/>
10.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	<input type="checkbox"/>	<input type="checkbox"/>
10.7	Ensure Public Network Access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.5	Ensure that 'System Assigned Managed Identity' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure that 'Public Network Access' is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.6	Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	<input type="checkbox"/>	<input type="checkbox"/>
10.7	Ensure Public Network Access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure 'Microsoft Entra Authentication' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure that 'Allow access only via SSL' is set to 'Yes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure that 'Minimum TLS version' is set to TLS v1.2 (or higher)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure that 'System Assigned Managed Identity' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure that 'Public Network Access' is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure That Private Endpoints Are Used Where Possible	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Use Entra ID Client Authentication and Azure RBAC where possible.	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Ensure 'TLS Version' is set to 'TLSV1.2' (or higher) for MySQL flexible Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.6	Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	<input type="checkbox"/>	<input type="checkbox"/>
7.8	Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Single Server Only)	<input type="checkbox"/>	<input type="checkbox"/>
10.1	Ensure that 'Auditing' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	<input type="checkbox"/>	<input type="checkbox"/>
10.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	<input type="checkbox"/>	<input type="checkbox"/>
10.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	<input type="checkbox"/>	<input type="checkbox"/>
10.7	Ensure Public Network Access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Ensure 'Microsoft Entra Authentication' is 'Enabled'	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure that 'Allow access only via SSL' is set to 'Yes'	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure that 'Minimum TLS version' is set to TLS v1.2 (or higher)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure that 'Access Policies' are implemented and reviewed periodically	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Ensure that 'System Assigned Managed Identity' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Ensure that 'Public Network Access' is 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure That Private Endpoints Are Used Where Possible	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Use Entra ID Client Authentication and Azure RBAC where possible.	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Ensure 'TLS Version' is set to 'TLSV1.2' (or higher) for MySQL flexible Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
7.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.6	Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	<input type="checkbox"/>	<input type="checkbox"/>
7.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled	<input type="checkbox"/>	<input type="checkbox"/>
7.8	Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Single Server Only)	<input type="checkbox"/>	<input type="checkbox"/>
10.1	Ensure that 'Auditing' is set to 'On'	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	<input type="checkbox"/>	<input type="checkbox"/>
10.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	<input type="checkbox"/>	<input type="checkbox"/>
10.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database	<input type="checkbox"/>	<input type="checkbox"/>
10.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	<input type="checkbox"/>	<input type="checkbox"/>
10.7	Ensure Public Network Access is Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8.0	<input type="checkbox"/>	<input type="checkbox"/>