**CORE SERVICE DESIGN:**

**Azure SQL Database**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Dominic Panzera |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure SQL Database Core Service Design |
| **File Name** | Ambulance Victoria – Azure SQL Database Core Service Design v2.0.docx |
| **Version** | 2.0 |
| **Status** | Updated |
| **Release Date** | 28/02/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Dileep Pradeep |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 15/02/2024 |
| 2.0 | Updated | Minor feedback | 10, 14-17, 21-25 | 28/02/2024 |

Table of Contents

[1. Overview 5](#_Toc160006021)

[1.1 Purpose and Audience 5](#_Toc160006022)

[1.2 Scope and Key Deliverables 5](#_Toc160006023)

[1.3 Glossary and Definitions 6](#_Toc160006024)

[2. Executive Summary 7](#_Toc160006025)

[3. Resource Cost 8](#_Toc160006026)

[4. WAF and Security Control Alignment 8](#_Toc160006027)

[4.1 Reliability 9](#_Toc160006028)

[4.1.1 Overview 9](#_Toc160006029)

[4.1.2 Azure SQL Database Reliability Checklist 9](#_Toc160006030)

[4.2 Cost Optimisation 10](#_Toc160006031)

[4.2.1 Overview 10](#_Toc160006032)

[4.2.2 Azure SQL Database Cost Optimisation Checklist 10](#_Toc160006033)

[4.3 Operational Excellence 10](#_Toc160006034)

[4.3.1 Overview 10](#_Toc160006035)

[4.3.2 Azure SQL Database Operational Excellence Checklist 11](#_Toc160006036)

[4.4 Performance Efficiency 11](#_Toc160006037)

[4.4.1 Overview 11](#_Toc160006038)

[4.4.2 Azure SQL Database Performance Efficiency Checklist 11](#_Toc160006039)

[4.5 Security 12](#_Toc160006040)

[4.5.1 Overview 12](#_Toc160006041)

[5. Architecture Summary 13](#_Toc160006042)

[5.1 Resource Overview 13](#_Toc160006043)

[5.1.1 Service Tiers 14](#_Toc160006044)

[5.1.2 Elastic Pools 14](#_Toc160006045)

[5.1.3 Geo-replication and Auto failover 14](#_Toc160006046)

[5.2 RBAC 16](#_Toc160006047)

[5.3 Design Decisions and Justifications 16](#_Toc160006048)

[5.3.1 Service Tier 17](#_Toc160006049)

[5.3.2 Geo-Replication 17](#_Toc160006050)

[5.3.3 Auto-failover Groups 17](#_Toc160006051)

[5.3.4 Zone-Redundant Databases 17](#_Toc160006052)

[5.3.5 SQL Analytics and Monitoring 18](#_Toc160006053)

[5.3.6 Compute tier 18](#_Toc160006054)

[5.3.7 Tuning 18](#_Toc160006055)

[5.3.8 Network Access 19](#_Toc160006056)

[5.3.9 Elastic Pools 19](#_Toc160006057)

[5.3.10 Threat Detection 19](#_Toc160006058)

[5.3.11 Authentication 19](#_Toc160006059)

[5.3.12 Administrator Account 20](#_Toc160006060)

[5.3.13 Encryption 20](#_Toc160006061)

[5.3.14 Logging and Monitoring 20](#_Toc160006062)

[5.3.15 Automated Backups 20](#_Toc160006063)

[6. Azure Policies 21](#_Toc160006064)

[7. Configuration Templates 21](#_Toc160006065)

[7.1 Primary Region Platinum Azure SQL Database 21](#_Toc160006066)

[7.2 Secondary Region Platinum Azure SQL Database 23](#_Toc160006067)

[7.3 Primary Region Gold/Silver Azure SQL Database 23](#_Toc160006068)

[7.4 Primary Region Bronze Azure SQL Database 25](#_Toc160006069)

[8. Acceptance 25](#_Toc160006070)

# Overview

This document covers the baseline design for the Azure SQL Database core service. The intention of this document is to define the overall resource design in isolation from a specific application. It is aimed to highlight the general process and requirements for building a Azure SQL Database in a repeatable fashion with consistent configurations. Design decisions and justifications have been included in the Architecture section, and this document can be used as a reference for new builds that require a Azure SQL Database.

This design caters to a Level 2 design which covers both Microsoft’s WAF (Well Architected Framework)[[1]](#footnote-2) and the Department of Health Control list.

Any deviations required to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum if they are required for any reason for a specific build.

## Purpose and Audience

This document will outline the standard design and configuration of this Azure service in Ambulance Victoria’s Azure tenancy as a baseline for any application infrastructure deployments.

This design is intended to:

* Meet Microsoft WAF standards.
* Meet the controls stipulated by the Department of Health.
* Define the baseline required for the deployment of the resource.

The audience for this document is those involved in the planning, designing, and implementing of the Application/Data infrastructure. This includes:

* + Ambulance Victoria IT staff

It is assumed that the reader knows and is familiar with Azure Cloud concepts and related topics.

## Scope and Key Deliverables

The scope of this core service design is to define the baseline deployment requirements and standards for the Azure SQL Database core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |

Table 1: Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Azure SQL Database Core Service. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

This section contains a summary of the major design decisions that have been made for defining the baseline of this resource as an outcome of the WAF and Security analysis detailed throughout this document.

Of the five WAF Pillars, it was found that Reliability, Performance Efficiency Cost Optimisation and Security were relevant.

For this service the main baseline configurations include:

* All will use the same hardware (Standard series), unless a Premium hardware is specifically required for an application.
* Zone-redundancy is not available in Australia Southeast so is not applicable to any deployment.
* Public access will be disabled, and private endpoints will be used instead.
* Defender for SQL will be enabled across all resources.

There are some notable differences across the service tier configurations for this service:

* Platinum, Gold and Silver will use the Business Critical tier, and Non-Production will use the General Purpose tier
* Geo-replication will be used for Production workloads, and locally redundant will be used for Non-Production

# Resource Cost

Azure SQL Database is priced as follows, assuming a Standard series database using a vCore purchasing model[[2]](#footnote-3):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Min vCores | Max vCores | Min Memory (GB) | Max Memory (GB) | Price |
| 0.5 | 80 | 2.05 | 240 | **$0.0001896**/vCore-second (**$0.683**/vCore-hour) |

Table 2: Pricing for Azure SQL database

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Azure SQL Database Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Use Active Geo-Replication to create a readable secondary in a different region. | Yes | Yes | IaC | At deployment |
| **R2** | Use Auto Failover Groups that can include one or multiple databases, typically used by the same application. | Yes | Yes | Governance | Operational – during Application design |
| **R3** | Use a Zone-Redundant database. | No | No | N/A | N/A |
| **R4** | Monitor your Azure SQL Database in near-real time to detect reliability incidents. | Yes | Yes | IaC – SQL DB module | At deployment |
| **R5** | Implement Retry Logic. | Yes | No | Governance | Operational – during Application design |

Table 3: WAF Reliability checklist summary

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[4]](#footnote-5). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Azure SQL Database Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Optimize queries. | Yes | No | Governance | Operational |
| **CO2** | Evaluate resource usage. | Yes | No | Governance | Operational – during application deployment, review monthly |
| **CO3** | Fine-tune backup storage consumption | Yes | No | Governance | Operational – review quarterly |
| **CO4** | Evaluate Azure SQL Database Serverless. | Yes | No | Governance | Operational – during application design |
| **CO5** | Consider reserved capacity for Azure SQL Database. | Yes | No | Governance | Operational – review quarterly |
| **CO6** | Elastic pools help you manage and scale multiple databases in Azure SQL Database | Yes | Yes | IaC | At deployment |

Table 4: WAF Cost Optimisation checklist summary

## Operational Excellence

### Overview

Operational Excellence aims to ensure that once the architecture is built, the ongoing operations are flawless. This includes repeatable and reliable deployments, automating to eliminate human error. To do this the following must be considered:

* Optimise the build and release process (including CI/CD and IaC)
* Understand Operational Health
* Test recovery and failure
* Focus on continuous improvement
* Use loosely coupled architecture

### Azure SQL Database Operational Excellence Checklist

The guidance for operational excellence is identical to Performance Efficiency so has not been repeated here.

## Performance Efficiency

### Overview

Performance Efficiency refers to the ability of your systems and applications to meet user demands without breaking or creating a negative user experience[[5]](#footnote-6). This covers capacity and scalability:

* Design for horizontal scaling
* Run stress and performance tests
* Continuously monitor performances, particularly in Production systems

### Azure SQL Database Performance Efficiency Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **PE1** | Diagnose and troubleshoot high CPU utilization. | Yes | No | Governance | Operational – review as required |
| **PE2** | Understand blocking and deadlocking issues. | Yes | No | Governance | Operational |
| **PE3** | Tune applications and databases for performance. | Yes | No | Governance | Operational – at deployment |
| **PE4** | Review Azure portal utilization reporting and scale as appropriate. | Yes | No | Governance | Operational – review monthly |
| **PE5** | Review Performance Recommendations. | Yes | No | Governance | Operational – review monthly |
| **PE6** | Review Query Performance Insight. | Yes | No | Governance | Operational – review monthly |
| **PE7** | Configure Automatic tuning. | Yes | No | Governance | Operational – at deployment |
| **PE8** | Evaluate potential use of in-memory database objects. | Yes | No | Governance | Operational – review monthly |
| **PE9** | Leverage the Query Store. | Yes | No | Governance | Operational |
| **PE10** | Implement retry logic for transient errors. | Yes | No | Governance | Operational – during application design |

Table 6: WAF Performance Efficiency checklist summary

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[6]](#footnote-7):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark Controls are applicable:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* IM-1: Use centralized identity and authentication system
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* LT-1: Enable threat detection capabilities
* LT-3: Enable logging for security investigation
* LT-4: Enable logging for security investigation
* BR-1: Ensure regular automated backups

# Architecture Summary

## Resource Overview

Azure SQL Database is a PaaS service offering that operates as a database engine and handles most of the underlying infrastructure functions such as upgrading, patching, backup and monitoring[[7]](#footnote-8). It will always operate on the latest stable version of SQL database engine with 99.99% availability.

### Service Tiers

There are several service tiers for the Core-based purchasing model:

* General Purpose
* Business Critical
* Hyperscale

General Purpose is applicable to most common workloads, and balances price with compute and storage options.

Business Critical is for applications that have high-transaction rates and low latency requirements.

Hyperscale is designed for business workloads that require the most flexibility and highest performance. It also offers resilience to failure by allowing more than one isolated database replica.

### Elastic Pools

Elastic Pools are a feature of Azure SQL Database that allows you to manage and scale multiple databases which may have varied and unpredictable usage. The databases on an elastic pool are placed on a single server with a set price.

### Geo-replication and Auto failover

With respect to Disaster Recovery for Azure SQL Databases, there are two major components[[8]](#footnote-9):

* Geo-replication
* Failover Groups

Geo-replication is the feature that continuously replicates data from the primary SQL Database to a readable secondary database. This secondary database may be in the same region, but it is typically recommended to host this in a separate region to protect against regional outages.

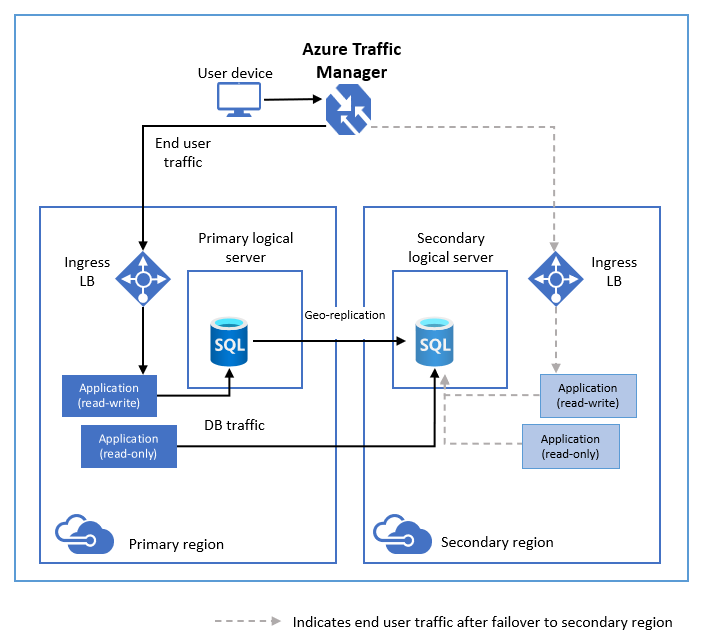


Figure 1: Geo-replication example

Geo-replication is a settings that is enabled per database, and only supports manual failover. To failover multiple databases together, a Failover Group is required.

Failover Groups allow you to manage the replication and failover of all databases hosted on a logical server to a secondary logical server in another region. An important feature of this is that the secondary databases in the failover group can also be used to offload read-only workloads, which reduces traffic to the primary database.

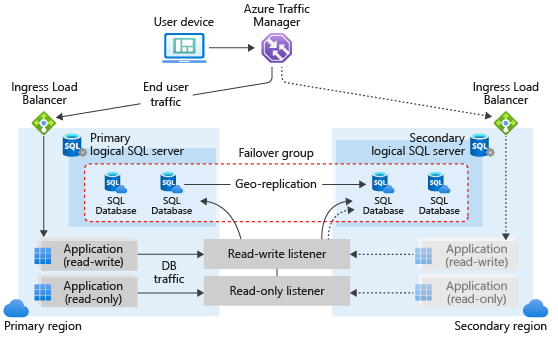


Figure 2: Geo-replication with Failover Groups

## RBAC

For the Azure SQL Database, the following roles are applicable[[9]](#footnote-10):

|  |  |
| --- | --- |
| Role Name | Description |
| SQL DB Contributor | Lets you manage SQL databases, but not access to them. Also, you can't manage their security-related policies or their parent SQL servers. |
| SQL Security Manager | Lets you manage the security-related policies of SQL servers and databases, but not access to them. |
| SQL Server Contributor | Lets you manage SQL servers and databases, but not access to them, and not their security-related policies. |

Table 8: RBAC roles relevant for this core service

## Design Decisions and Justifications

This section covers the design decisions and justifications that reflect the findings of the WAF and Security alignment. This will form the baseline requirements for the Azure SQL Database core service and will be captured in the accompanying Configuration Template with a set of pre-approved deployment settings for this resource. Any changes, modifications or removals to the pre-approved deployments must have specific approval from the Cloud Governance Forum prior to deployment.

### Service Tier

**Design Reference:** N/A

**Design Decision:** Business Critical will be used for Platinum databases that require low latency and high availability. General Purpose will be used for all other tiers.

**Design Justification:** Business Critical tier caters to applications that have intensive requirements for availability and latency, with better backup, storage type, and availability than the other tiers. As such it should be applied to Production workloads.

General Purpose is suitable for most business workloads, so can be applied to any database that does not require Business Critical, so Non-Production will utilise this.

Hyperscale can be used if specifically required, though it does not offer better performance or redundancy than the other tiers.

### Geo-Replication

**Design Reference:** Table 3- [R1](#_Azure_SQL_Database)

**Design Decision**: Geo-Replication will be used for Platinum workloads and can be optional for Gold/Silver workloads if required by the application. It is not required for Bronze workloads.

**Design Justification**: Geo-Replication ensures redundancy for the workloads. It comes at a higher cost than locally redundant replication. As such it is recommended that this is the default option for Platinum workloads. It can be optional for Gold/Silver workloads should the application require this. It is not needed for Bronze workloads or Non-Production.

### Auto-failover Groups

**Design Reference:** Table 3- [R2](#_Azure_SQL_Database)

**Design Decision:** Failover Groups will be used by Production workloads, particularly Platinum. It will not be used for Non-Production.

**Design Justification:** Failover Groups will not be enabled by default as they are a function of a specific application or set of databases that can be failed over together. This needs to be defined as a part of application design, but should be used where possible for additional redundancy, particularly for Platinum applications.

### Zone-Redundant Databases

**Design Reference:** Table 3- [R3](#_Azure_SQL_Database)

**Design Decision:** Availability zones are not currently available in Australia Southeast so cannot be enabled. They should be enabled once they become Generally Available for Production workloads.

**Design Justification:** Availability zones guarantee a higher level of availability in case one Data Centre is unavailable. Currently this is not an option in the primary region, however, should be enabled once it becomes available, primarily for Platinum workloads. It can be considered for Gold/Silver if required by the application.

### SQL Analytics and Monitoring

**Design Reference:** Table 3- [R4](#_Azure_SQL_Database)

**Design Decision:** Azure SQL Analytics is in public preview so will not be enabled, but should be considered when it becomes generally available. Monitoring logs will be sent to the central log analytics workspace.

**Design Justification:** Azure SQL Analytics is in public preview so should not be enabled as it is not generally available and may not function properly, and has no SLA from Microsoft. It should be considered when it becomes Generally Available.

As standard for monitoring all resources, AllLogs and allMetrics will be sent to the central log analytics workspace in that region.

### Compute tier

**Design Reference:** Table 4 – [CO4](#_Azure_SQL_Database_1)

**Design Decision:** Use Azure SQL Database Serverless over Provisioned Compute Tier

**Design Justification:** Azure SQL Database Serverless tier is a compute tier that will automatically scale compute based on workload demands. However, this is not recommended for all scenarios, such as unpredictable or burstable patterns. In these cases, the Provisioned Compute Tier may be optimal. This should be defined during the application design.

### Tuning

**Design Reference:** Table 6 – [PE7,PE3](#_Azure_SQL_Database_3)

**Design Decision:** Autotuning will be enabled at deployment. Any other form of manual tuning.

**Design Justification:** Enabling autotuning must be done through the Azure Portal for each database and will help automatically optimise database performances. Any other form of tuning must be done manually by the DBA team.

### Network Access

**Design Reference:** Microsoft Security Benchmark [NS-1, NS-2](#_Azure_SQL_Database_2)

**Design Decision:** Disable Public Access and use Private Link for access to Azure SQL Database.

**Design Justification:** Private Link is the most secure form of connectivity for Azure SQL Database. If there is a reason it cannot be used it is recommended to use Service Endpoints instead. Public access should be disabled by default. Network Rules on the instance should be added to the server to allow only from specific networks that require access to it.

### Elastic Pools

**Design Reference:** Table 4 – [CO6](#_Azure_SQL_Database_1)

**Design Decision:** Elastic Pools will be used if required by an application, or if multiple databases can be shared on a single host.

**Design Justification:** Elastic Pools help to optimise costs by allowing multiple databases to share a set of underlying resources at a fixed price. This may not be suitable for all databases and can be enabled during creation of the Azure SQL Database. It is important to review which databases can share the same underlying infrastructure before implementing. The elastic pool configuration follows the same requirements as the standard database settings in terms of tier and compute hardware.

### Threat Detection

**Design Reference:** Microsoft Security Benchmark [LT-1](#_Overview)

**Design Decision:** Microsoft Defender for Azure SQL will be enabled.

**Design Justification:** Microsoft Defender for Azure SQL handles vulnerability assessments on databases as well as threat protection based on SQL Advanced Threat Protection.

### Authentication

**Design Reference:** Microsoft Security Benchmark – [IM-1](#_Azure_SQL_Database_2)

**Design Decision:** Azure AD Authentication (now Microsoft Entra ID) will be used for access to Azure SQL Databases. Local Authentication should be disabled.

**Design Justification:** Microsoft Entra ID will be configured as the baseline authentication method. It is more secure than local authentication methods which do not require MFA and have a higher risk of compromise.

### Administrator Account

**Design Reference:** Microsoft Security Benchmark [IM-1](#_Overview)

**Design Decision:** Azure AD Groups will be used to assign the SQL Server Admin role instead of direct assignments.

**Design Justification:** As is the standard for role assignments, a Group should be assigned the admin role for the SQL server administrator. It simplifies permissions management, particularly when offboarding users, they simply should be removed from the groups they are assigned to instead of multiple individual resources.

### Encryption

**Design Reference:** Microsoft Security Benchmark [DP3, DP4](#_Azure_SQL_Database_3)

**Design Decision:** Encryption at rest is enabled by default. The minimum TLS version will be set to 1.2. Transparent Data encryption will also be enabled for database level encryption.

**Design Justification:** Encryption of infrastructure is a default setting, so at rest is already encrypted by default. TLS will be set to a minimum of 1.2 as is the industry standard, preferentially to weaker encryption levels of 1.0 and 1.1. Additionally, to secure database level files, Transparent Data Encryption will also be enabled.

### Logging and Monitoring

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Overview)

**Design Decision:** Auditing will be enabled on SQL Server. Diagnostic logs will be sent to the central log analytics workspace for that region.

**Design Justification:** Auditing on SQL Server Database allows you to track database activities and have them saved in audit logs, allowing you to identify potentially malicious changes more easily. Logging as a security and compliance requirement will be met by sending allLogs and allMetrics to the central log analytics workspace for that region.

### Automated Backups

**Design Reference:** Microsoft Security Benchmark [BT-1](#_Overview)

**Design Decision:** The native backup solution for Azure SQL Database will be leveraged.

**Design Justification:** Until an overall backup solution is implemented, the simplest solution is to configure backups to take place locally through the Azure SQL Database service. It will create by default:

* Full backups every week.
* Differential backups every 12 or 24 hours.
* Transaction log backups approximately every 10 minutes.

# Azure Policies

The following policies should be applied to audit or enforce the configurations for Azure SQL Database:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Private endpoint connections on Azure SQL Database should be enabled | av (root management group) |
| Public network access on Azure SQL Database should be disabled | av (root management group) |
| An Azure Active Directory administrator should be provisioned for SQL servers | av (root management group) |
| Azure SQL Database should have Azure Active Directory Only Authentication enabled | av (root management group) |
| Transparent Data Encryption on SQL databases should be enabled | av (root management group) |
| Auditing on SQL server should be enabled | av (root management group) |

Table 9: Azure Policies

# Configuration Templates

## Primary Region Platinum Azure SQL Database

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sqldb-prd-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Workload Environment** | Production |
| **SQL Database Server name** | sql-prd-ause-[appname]-01 |
| **Authentication Method** | Microsoft Entra ID only |
| **Service Tier** | Business Critical |
| **Hardware Configuration** | Standard Series (Gen5) |
| **vCores** | 2-128 GB |
| **Data max size (GB)** | 32-4096 GB |
| **Backup storage redundancy** | Geo-Redundant backup storage |
| **Connectivity Method** | Private Endpoint |
| **Connection Policy** | Default |
| **Encrypted Connections** | Minimum TLS 1.2 |
| **Enable Microsoft Defender for SQL** | Enabled |
| **Server Identity** | Managed Identity enabled |
| **Transparent Data Encryption** | Enabled – server level key |
| **Maintenance Window** | 10pm – 6am AU Standard Time Friday to Sunday |
| **Auditing** | Enable to Log Analytics Workspace |
| ***Failover Group and Secondary Instance Settings*** | |
| **Failover Group Name** | fgprdause[appname]01 |
| **Secondary Server** | sqldb-dr-auea-[appname]-01 |
| **Secondary Server Region** | Australia East |
| ***Private Endpoint Settings*** |  |
| **Name** | pep-sql-prd-ause-[appname]-01 |
| **Virtual Network** | vnet-prd-ause-[appname]-01 |
| **Subnet** | snet-prd-ause-[appname]-db-01 |
| **Private DNS Zone** | privatelink.database.windows.net |
| ***(Optional) Elastic Pool Settings*** |  |
| **Name** | sqlep-prd-ause-[appname]-01 |
| **Service Tier** | Business Critical |
| **Hardware Configuration** | Standard Series (Gen5) |
| **vCores** | 4-128 GB |
| **Data max size (GB)** | 1-4096 GB |
| **Per Database settings** | 0.25-128 vCores |

## Secondary Region Platinum Azure SQL Database

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sqldb-dr-auea-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Workload Environment** | Production |
| **SQL Database Server name** | sql-dr-auea-[appname]-01 |
| **Authentication Method** | Microsoft Entra ID only |
| **Service Tier** | General Purpose |
| **Hardware Configuration** | Standard Series (Gen5) |
| **vCores** | 2-128 GB |
| **Data max size (GB)** | 32-4096 GB |
| **Backup storage redundancy** | Locally-Redundant backup storage |
| **Connectivity Method** | Private Endpoint |
| **Connection Policy** | Default |
| **Encrypted Connections** | Minimum TLS 1.2 |
| **Enable Microsoft Defender for SQL** | Enabled |
| **Server Identity** | Managed Identity enabled |
| **Transparent Data Encryption** | Enabled – server level key |
| **Maintenance Window** | 10pm – 6am AU Standard Time Friday to Sunday |
| **Auditing** | Enable to Log Analytics Workspace |
| ***Private Endpoint Settings*** |  |
| **Name** | pep-sql-dr-auea-[appname]-01 |
| **Virtual Network** | vnet-prd-auea-[appname]-01 |
| **Subnet** | snet-prd-auea-[appname]-db-01 |
| **Private DNS Zone** | privatelink.database.windows.net |

## Primary Region Gold/Silver Azure SQL Database

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sqldb-prd-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Workload Environment** | Production |
| **SQL Database Server name** | sql-prd-ause-[appname]-01 |
| **Authentication Method** | Microsoft Entra ID only |
| **Service Tier** | Business Critical |
| **Hardware Configuration** | Standard Series (Gen5) |
| **vCores** | 2-128 GB |
| **Data max size (GB)** | 32-4096 GB |
| **Backup storage redundancy** | Geo-Redundant backup storage |
| **Connectivity Method** | Private Endpoint |
| **Connection Policy** | Default |
| **Encrypted Connections** | Minimum TLS 1.2 |
| **Enable Microsoft Defender for SQL** | Enabled |
| **Server Identity** | Managed Identity enabled |
| **Transparent Data Encryption** | Enabled – server level key |
| **Maintenance Window** | 10pm – 6am AU Standard Time Friday to Sunday |
| **Auditing** | Enable to Log Analytics Workspace |
| ***Failover Group and Secondary Instance Settings*** | |
| **Failover Group Name** | fgprdause[appname]01 |
| **Secondary Server** | sqldb-dr-auea-[appname]-01 |
| **Secondary Server Region** | Australia East |
| ***Private Endpoint Settings*** |  |
| **Name** | pep-sql-prd-ause-[appname]-01 |
| **Virtual Network** | vnet-prd-ause-[appname]-01 |
| **Subnet** | snet-prd-ause-[appname]-db-01 |
| **Private DNS Zone** | privatelink.database.windows.net |
| ***(Optional) Elastic Pool Settings*** |  |
| **Name** | sqlep-prd-ause-[appname]-01 |
| **Service Tier** | Business Critical |
| **Hardware Configuration** | Standard Series (Gen5) |
| **vCores** | 4-128 GB |
| **Data max size (GB)** | 1-4096 GB |
| **Per Database settings** | 0.25-128 vCores |

## Primary Region Bronze Azure SQL Database

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sqldb-[env]-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Workload Environment** | Non-Production |
| **SQL Database Server name** | sql-[env]-ause-[appname]-01 |
| **Authentication Method** | Microsoft Entra ID only |
| **Service Tier** | General Purpose |
| **Hardware Configuration** | Standard Series (Gen5) |
| **vCores** | 2-128 GB |
| **Data max size (GB)** | 32-4096 GB |
| **Backup storage redundancy** | Locally-redundant backup storage |
| **Connectivity Method** | Private Endpoint |
| **Connection Policy** | Default |
| **Encrypted Connections** | Minimum TLS 1.2 |
| **Enable Microsoft Defender for SQL** | Enabled |
| **Server Identity** | Managed Identity enabled |
| **Transparent Data Encryption** | Enabled – server level key |
| **Maintenance Window** | 5pm – 8am |
| **Auditing** | Enable to Log Analytics Workspace |
| ***Private Endpoint Settings*** |  |
| **Name** | pep-sql-[env]-ause-[appname]-01 |
| **Virtual Network** | vnet-[env]-ause-[appname]-01 |
| **Subnet** | snet-[env]-ause-[appname]-db-01 |
| **Private DNS Zone** | privatelink.database.windows.net |

# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://azure.microsoft.com/en-us/pricing/details/azure-sql-database/single/ [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/azure-sql/database/sql-database-paas-overview?view=azuresql [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview?view=azuresql [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-10)