**CORE SERVICE DESIGN:**

**Azure SQL Managed Instance**

atabricks

SQL admin

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure SQL Managed Instance Core Service Design |
| **File Name** | Ambulance Victoria – Azure SQL Managed Instance Core Service Design v3.0.docx |
| **Version** | 3.0 |
| **Status** | Released |
| **Release Date** | 29/02/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 22/02/2024 |
| 2.0 | Updated | Minor feedback | 14, 20-22 | 28/02/2024 |
| 3.0 | Updated | Network Segmentation | 7, 13, 17 | 29/02/2024 |

Table of Contents

[1. Overview 5](#_Toc160096812)

[1.1 Purpose and Audience 5](#_Toc160096813)

[1.2 Scope and Key Deliverables 5](#_Toc160096814)

[1.3 Glossary and Definitions 6](#_Toc160096815)

[2. Executive Summary 7](#_Toc160096816)

[3. Resource Cost 8](#_Toc160096817)

[4. WAF and Security Control Alignment 8](#_Toc160096818)

[4.1 Reliability 9](#_Toc160096819)

[4.1.1 Overview 9](#_Toc160096820)

[4.1.2 Azure SQL Managed Instance Reliability Checklist 9](#_Toc160096821)

[4.2 Cost Optimisation 10](#_Toc160096822)

[4.2.1 Overview 10](#_Toc160096823)

[4.2.2 Azure SQL Managed Instance Cost Optimisation Checklist 10](#_Toc160096824)

[4.3 Operational Excellence 10](#_Toc160096825)

[4.3.1 Overview 10](#_Toc160096826)

[4.3.2 Azure SQL Managed Instance Operational Excellence Checklist 10](#_Toc160096827)

[4.4 Performance Efficiency 11](#_Toc160096828)

[4.4.1 Overview 11](#_Toc160096829)

[4.5 Security 12](#_Toc160096830)

[4.5.1 Overview 12](#_Toc160096831)

[5. Architecture Summary 13](#_Toc160096832)

[5.1 Resource Overview 13](#_Toc160096833)

[5.1.1 Networking Requirements 13](#_Toc160096834)

[5.1.2 Service Tiers 14](#_Toc160096835)

[5.1.3 Auto-failover 14](#_Toc160096836)

[5.2 RBAC 15](#_Toc160096837)

[5.3 Design Decisions and Justifications 16](#_Toc160096838)

[5.3.1 Tier Selection 16](#_Toc160096839)

[5.3.2 Compute Tier Selection 16](#_Toc160096840)

[5.3.3 Auto-failover 16](#_Toc160096841)

[5.3.4 Network Connectivity 17](#_Toc160096842)

[5.3.5 Authentication 17](#_Toc160096843)

[5.3.6 Administrator Account 17](#_Toc160096844)

[5.3.7 Identity 17](#_Toc160096845)

[5.3.8 Encryption 18](#_Toc160096846)

[5.3.9 Threat Detection 18](#_Toc160096847)

[5.3.10 Logging and Monitoring 18](#_Toc160096848)

[5.3.11 Backup 18](#_Toc160096849)

[6. Azure Policies 19](#_Toc160096850)

[7. Configuration Templates 20](#_Toc160096851)

[7.1 Primary Production SQL Managed Instance 20](#_Toc160096852)

[7.2 Secondary Production SQL Managed Instance for Failover 21](#_Toc160096853)

[7.3 Primary Non-Production SQL Managed Instance 22](#_Toc160096854)

[8. Acceptance 23](#_Toc160096855)

# Overview

This document covers the baseline design for the Azure SQL Managed Instance 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 Managed Instance 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 Managed Instance.

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 Managed Instance 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 : Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Azure SQL Managed Instance 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 and Security were relevant. The Operational Excellence guidance was identical to the Reliability guidance so has not been repeated in this document.

For this service the main baseline configurations include:

* Standard-series hardware will be used for all deployments as the default
* Authentication will be Microsoft Entra ID only
* SQL Administrator Accounts will be assigned through RBAC groups
* Managed Identities will be used instead of Service Principals
* TLS will be set to a minimum of 1.2
* Transparent Data Encryption will be enabled
* The Instances must be deployed into a subnet dedicated to Managed Instances. This is a requirement and supports the network segmentation strategy.

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

* Business Critical tier will be used for Production, and General Purpose will be used for Non-Production.
* Backup redundancy will be Geo-redundant for Platinum workloads, optionally Geo-redundant for Gold/Silver workloads, and Locally redundant for Non-Production workloads.
* Production workloads will have a secondary Managed Instance for auto-failover

# Resource Cost

The following is the pricing construct for Azure SQL Managed Instance assuming the Standard-series compute under the Business Critical tier[[2]](#footnote-3):

|  |  |  |  |
| --- | --- | --- | --- |
| vCORE | Memory (GB) | Included Storage | Pay as you go |
| 4 | 20.4 | First 32 GB/month | $4.474/hour |
| 8 | 40.8 | First 32 GB/month | $8.947/hour |
| 16 | 81.6 | First 32 GB/month | $17.894/hour |
| 24 | 122.4 | First 32 GB/month | $26.841/hour |
| 32 | 163.2 | First 32 GB/month | $35.788/hour |
| 40 | 204 | First 32 GB/month | $44.735/hour |
| 64 | 326.4 | First 32 GB/month | $71.575/hour |
| 80 | 396 | First 32 GB/month | $89.469/hour |

Table : Pricing construct for SQL Managed Instance

There are costs associated with storage beyond the first 32 GB per month: month:

|  |  |
| --- | --- |
| Storage | Price |
| First 32 GB/instance/month | Included |
| Additional storage\* | $0.210/GB/month |

Table : Pricing construct for additional storage

# 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 Managed Instance Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Use the Business Critical Tier. | Yes | Yes | IaC | At deployment |
| **R2** | Configure a secondary instance and an Autofailover group to enable failover to another region. | Yes | Yes | IaC | At deployment |
| **R3** | Implement Retry Logic. | Yes | No | Governance | Operational – during application design |
| **R4** | Monitor your SQL MI instance in near-real time to detect reliability incidents. | Yes | Yes | Operational | Operational – enable On-Prem monitoring in addition to Azure Monitor |

Table : 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 Managed Instance Cost Optimisation Checklist

There is no guidance for Azure SQL Managed Instance under Cost Optimisation.

## 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 Managed Instance Operational Excellence Checklist

The guidance for Azure SQL Managed Instance under Operational Excellence was identical to Reliability so it has not been repeated.

## 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

There is no guidance for Azure SQL Managed Instance under Performance Efficiency.

## 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
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default

# Architecture Summary

## Resource Overview

Azure SQL Managed Instance is a fully managed PaaS service that is compatible with the latest Enterprise Edition SQL Server database engine[[7]](#footnote-8). It allows you to lift and shift on-premises applications to the cloud with minimal application and database changes.

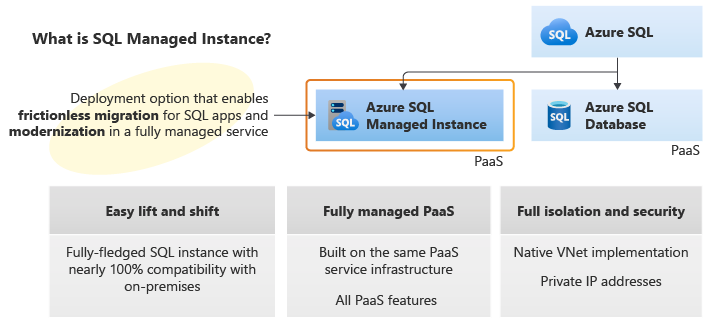
It combines features that are available on Azure SQL Database and the SQL server database engines.

Figure : Comparison of Azure SQL MI and Azure SQL DB

Though it is a lift and shift compatible PaaS service, there are some key differences between this and the classic SQL server On-Prem databases:

* High-Availability is built in and preconfigured
* Automated backups
* Microsoft Entra authentication is supported
* Connectivity is only supported through TCP, not through named pipes
* The instance can be started and stopped to save costs.

### Networking Requirements

Part of the overall strategy for applications and networking is to ensure segmentation, even within applications. This includes separating subnets for applications and databases. To deploy Managed Instances, a dedicated subnet is required, which must be delegated to the service provider for Managed Instances[[8]](#footnote-9). It must have at least 32 IP addresses available in the subnet.

### Service Tiers

There are two Service Tiers available for the Managed Instance:

* General Purpose – best for typical workloads with average performance and latency
* Business Critical – recommended for Production applications with low latency

### Auto-failover

Azure SQL Managed Instances can be configured with a secondary instance in the Disaster Recovery region for failover[[9]](#footnote-10). This secondary instance must be empty and is recommended to have the same configuration in terms of tiers and sizing as the primary instance. It is essentially an identical shell that can be used as the destination for failover in the event of an outage.

In the event of a primary region outage, Microsoft will initiate failover of any failover groups that have been configured with the Microsoft-managed failover policy. A customer managed policy, however, is recommended as this failover can be initiated at any time in case a single database is down and requires recovery instead of a full regional outage.

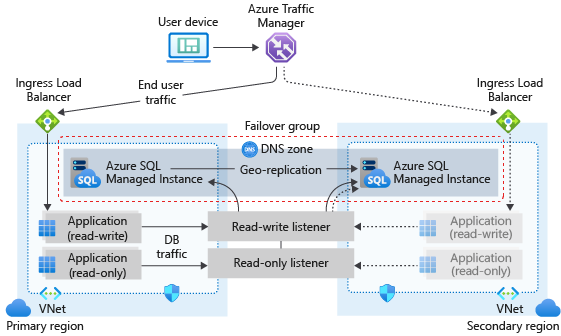


Figure : Typical failover architecture with SQL Managed Instance[[10]](#footnote-11)

Note that for the above scenarios the traffic manager and load balancers are used for application-layer requests, not to perform any failover mechanism for the instances. As mentioned it is recommended to failover using customer managed failover policies.

## RBAC

For the Azure SQL Managed Instance service, the specific roles that can be applied are as follows[[11]](#footnote-12):

|  |  |
| --- | --- |
| Role Name | Description |
| SQL Managed Instance Contributor | Lets you manage SQL Managed Instances and required network configuration, but can't give access to others. |
| SQL Security Manager | Lets you manage the security-related policies of SQL servers and databases, but not access to them. |

Table : 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 Managed Instance 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.

### Tier Selection

**Design Reference:** Table 4 – [R1](#_Azure_SQL_Managed)

**Design Decision**: the Business Critical Tier will be used for Production. The General Purpose tier will be used for Non-Production.

**Design Justification**: the Business Critical Tier provides higher resiliency to failure and fails over more quickly in the event of a disaster. It has better underlying High Availability architecture. As such it is recommended to use Business Critical for Production workloads, and Genera Purpose for less critical workloads.

### Compute Tier Selection

**Design Reference:** N/A

**Design Decision:** Standard-series will be used generally across all tiers, unless there is a specific application requirement for Premium tier hardware.

**Design Justification:** The Standard-series hardware is generally applicable to most applications, including Platinum workloads. The Premium and Premium (memory optimised) tiers should only be used when there is an incredibly high intensity database operational that requires lower latency and higher compute power. Otherwise, Standard will be the default.

### Auto-failover

**Design Reference:** Table 4 – [R2](#_Overview)

**Design Decision:** A secondary instance will be deployed for Production workloads.

**Design Justification:** To allow Auto-failover a secondary instance will be deployed in the Disaster Recovery region with the same tier and hardware tier configurations as the primary instance. The Failover Group policy will be set to customer managed. This is not required for Non-Production workloads.

### Network Connectivity

**Design Reference:** Microsoft Security Benchmark [NS-1](#_Azure_SQL_Managed_1)

**Design Decision:** Public endpoint (data) setting will be disabled.

**Design Justification:** By default, all public access should be disabled on services where applicable so that only private connectivity can establish a connection to the service.

Additionally, when the Managed Instances are deployed, they are deployed into a subnet that must be dedicated and delegated to the resource provider Microsoft.Sql/managedInstances.

### Authentication

**Design Reference:** Microsoft Security Benchmark [IM-1](#_Azure_SQL_Managed_1)

**Design Decision:** Microsoft Entra-only authentication will be used.

**Design Justification:** Using a centrally managed identity service for all authentication, which also requires users to MFA, provides more rigorous security surrounding the database access. It stops proliferation of user identities across database instances and allows you to manage database permissions using groups instead of direct assignments.Overall, it simplifies permissions management and increases security as compared to local SQL authentication.

### Administrator Account

**Design Reference:** Microsoft Security Benchmark [IM-1](#_Azure_SQL_Managed_1)

**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 permission management, particularly when offboarding users, they simply should be removed from the groups they are assigned to instead of multiple individual resources.

### Identity

**Design Reference:** Microsoft Security Benchmark [IM-3](#_Azure_SQL_Managed_1)

**Design Decision:** System assigned managed identity will be used instead of service principals. Service Principal authentication will be disabled.

**Design Justification:** The use of Managed Identities for authentication to Azure Services is more secure as Microsoft manage the automatic rotation of credentials, and guarantee that hard-coded credentials will be avoided.

### Encryption

**Design Reference:** Microsoft Security Benchmark [DP-3, DP-4](#_Overview)

**Design Decision:** Transparent Data Encryption will be enabled, and the Minimum TLS will be set to 1.2.

**Design Justification:** Data encryption at rest and in transit are security mandates. Data at-rest is enabled by default but will be bolstered by enabling the Transparent Data Encryption for the database layer. Additionally, encryption in transit will be made more secure by setting the Minimum TLS to be 1.2.

### Threat Detection

**Design Reference:** Microsoft Security Benchmark [LT-1](#_Azure_SQL_Managed_1)

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

**Design Justification:** Defender for SQL provides capability to identify potential vulnerabilities and can alert you to potentially malicious activities that could compromise the database.

### Logging and Monitoring

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Overview), Table 4 – [R4](#_Azure_SQL_Managed)

**Design Decision:** Logging will be enabled, and all logs and metrics sent to the log analytics workspace in that region. For Monitoring, Azure Monitor will be used. Note that there are additional SQL-specific monitoring agents that are in public preview – Azure SQL Insights and Azure SQL Analytics. It is recommended to enable these when they become Generally Available. For more detailed monitoring than Azure Monitor, it is recommended to enable any current Database Monitoring solutions on the Managed Instances.

**Design Justification:** It is a security and compliance requirement to have logs captured and retain centrally. As such the logs and metrics for each Azure SQL Managed Instance will be directed to the central log analytics workspace within the same region that the service is deployed.

### Backup

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

**Design Decision:** Redundancy will be Geo-redundant for Platinum and Production workloads, though optional for Gold/Silver depending on recovery and restore requirements. Locally-redundant will be used for Non-Production workloads.

**Design Justification:** For Platinum workloads Geo-redundancy is recommended to a secondary region to allow rapid restore in case the primary region is down. For Gold and Silver it may not be a requirement depending on the configuration of the application stack and RPO and RTO objectives, but it is recommended to use Geo-redundancy for Production workloads. Local redundancy is sufficient for Bronze and Non-Production workloads.

# Azure Policies

The following Azure policies should be applied:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Azure Defender for SQL should be enabled for unprotected SQL Managed Instances | av management group (under Root) |

Table : Azure Policies

# Configuration Templates

## Primary Production SQL Managed Instance

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sqlmi-prd-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Compute + storage** | Business Critical |
| **Hardware** | Standard-series (Gen 5) |
| **vCores** | 4-80 |
| **Storage in GB** | 32-1024 GB |
| **SQL Server License** | Pay-as-you-go |
| **Backup** | Geo-redundant |
| **Authentication** | Microsoft Entra ID (formerly Azure AD) |
| **Microsoft Entra Admin** | SQL Admin RBAC Group |
| **Virtual Network** | vnet-prd-ause-[appname]-01 |
| **Subnet** | snet-prd-ause-[appname]-[workload]-01 |
| **Connection Type** | Proxy (Default) |
| **Public endpoint** | Disable |
| **Minimum TLS** | 1.2 |
| **Enable Microsoft Defender for SQL** | Enabled |
| **Identity** | System Assigned Managed Identity |
| **Service principal** | Off |
| **Transparent Data Encryption** | Enabled - Service managed key |
| **Use as failover secondary** | No |
| **Maintenance window** | 10:00PM-6:AM Friday to Sunday |
| ***Failover Group and Secondary Instance Settings*** | |
| **Failover Group Name** | fgprdause[appname]01 |
| **Secondary Instance** | sqlmi-dr-auea-[appname]-01 |
| **Secondary Server Region** | Australia East |
| **Failover Policy** | Manual |
| **Failover Rights** | On |

## Secondary Production SQL Managed Instance for Failover

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sqlmi-dr-auea-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia East |
| **Compute + storage** | Business Critical |
| **Hardware** | Standard-series (Gen 5) |
| **vCores** | 4-80 |
| **Storage in GB** | 32-1024 GB |
| **SQL Server License** | Pay-as-you-go |
| **Backup** | Locally-redundant |
| **Authentication** | Microsoft Entra ID (formerly Azure AD) |
| **Microsoft Entra Admin** | SQL Admin RBAC Group |
| **Virtual Network** | vnet-dr-auea-[appname]-01 |
| **Subnet** | snet-dr-auea-[appname]-[workload]-01 |
| **Connection Type** | Proxy (Default) |
| **Public endpoint** | Disable |
| **Minimum TLS** | 1.2 |
| **Enable Microsoft Defender for SQL** | Enabled |
| **Identity** | System Assigned Managed Identity |
| **Service principal** | Off |
| **Transparent Data Encryption** | Enabled - Service managed key |
| **Use as failover secondary** | Yes |
| **Primary Managed Instance** | sqlmi-prd-ause-[appname]-01 |
| **Maintenance window** | 10:00PM-6:AM Friday to Sunday |

## Primary Non-Production SQL Managed Instance

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sqlmi-[env]-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Compute + storage** | General Purpose |
| **Hardware** | Standard-series (Gen 5) |
| **vCores** | 4-80 |
| **Storage in GB** | 32-1024 GB |
| **SQL Server License** | Pay-as-you-go |
| **Backup** | Locally redundant |
| **Authentication** | Microsoft Entra ID (formerly Azure AD) |
| **Microsoft Entra Admin** | SQL Admin RBAC Group |
| **Virtual Network** | vnet-[env]-ause-[appname]-01 |
| **Subnet** | snet-[env]-ause-[appname]-[workload]-01 |
| **Connection Type** | Proxy (Default) |
| **Public endpoint** | Disable |
| **Minimum TLS** | 1.2 |
| **Enable Microsoft Defender for SQL** | Enabled |
| **Identity** | System Assigned Managed Identity |
| **Service principal** | Off |
| **Transparent Data Encryption** | Enabled - Service managed key |
| **Use as failover secondary** | No |
| **Maintenance window** | 5:00PM-8:AM |

# 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-managed-instance/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/managed-instance/sql-managed-instance-paas-overview?view=azuresql [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/connectivity-architecture-overview?view=azuresql&tabs=current#service-aided-subnet-configuration-public-preview-in-east-us-and-west-us [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/failover-group-sql-mi?view=azuresql [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/failover-group-sql-mi?view=azuresql [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-12)