**CORE SERVICE DESIGN:**

**Service Bus**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Service Bus Core Service Design |
| **File Name** | Ambulance Victoria – Service Bus 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 | 22/02/2024 |
| 2.0 | Updated | Minor feedback | 14 | 28/02/2024 |

Table of Contents

[1. Overview 5](#_Toc159500519)

[1.1 Purpose and Audience 5](#_Toc159500520)

[1.2 Scope and Key Deliverables 5](#_Toc159500521)

[1.3 Glossary and Definitions 6](#_Toc159500522)

[2. Executive Summary 7](#_Toc159500523)

[3. Resource Cost 8](#_Toc159500524)

[4. WAF and Security Control Alignment 8](#_Toc159500525)

[4.1 Reliability 9](#_Toc159500526)

[4.1.1 Overview 9](#_Toc159500527)

[4.1.2 Service Bus Reliability Checklist 9](#_Toc159500528)

[4.2 Cost Optimisation 11](#_Toc159500529)

[4.2.1 Overview 11](#_Toc159500530)

[4.2.2 Service Bus Cost Optimisation Checklist 11](#_Toc159500531)

[4.3 Operational Excellence 11](#_Toc159500532)

[4.3.1 Overview 11](#_Toc159500533)

[4.3.2 Service Bus Operational Excellence Checklist 11](#_Toc159500534)

[4.4 Performance Efficiency 12](#_Toc159500535)

[4.4.1 Overview 12](#_Toc159500536)

[4.4.2 Service Bus Performance Efficiency Checklist 12](#_Toc159500537)

[4.5 Security 13](#_Toc159500538)

[4.5.1 Overview 13](#_Toc159500539)

[5. Architecture Summary 14](#_Toc159500540)

[5.1 Resource Overview 14](#_Toc159500541)

[5.2 RBAC 14](#_Toc159500542)

[5.3 Design Decisions and Justifications 15](#_Toc159500543)

[5.3.1 Service Tier 15](#_Toc159500544)

[5.3.2 Network Connectivity 15](#_Toc159500545)

[5.3.3 Authentication 15](#_Toc159500546)

[5.3.4 Encryption 16](#_Toc159500547)

[5.3.5 Geo-redundancy and High Availability 16](#_Toc159500548)

[5.3.6 Autoscaling 16](#_Toc159500549)

[5.3.7 Logging 16](#_Toc159500550)

[6. Azure Policies 17](#_Toc159500551)

[7. Configuration Templates 18](#_Toc159500552)

[7.1 Primary Region Production Service Bus Namespace 18](#_Toc159500553)

[7.2 Secondary Region Production Service Bus Namespace 18](#_Toc159500554)

[7.3 Primary Region Non-Production Service Bus Namespace 19](#_Toc159500555)

[8. Acceptance 21](#_Toc159500556)

# Overview

This document covers the baseline design for the Service Bus 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 Service Bus 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 Service Bus.

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 Service Bus 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 Service Bus 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, Operational Excellence and Security were relevant.

For this service the main baseline configurations include:

* Public access will be disabled and connectivity will take place through private endpoints
* All deployments will use the Premium tier (otherwise private endpoints cannot be used)
* Minimum TLS 1.2 will be configured
* Local Authentication will be disabled

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

* Geo-Disaster will be configured for Production workloads and is not required for Non-Production.

# Resource Cost

The following is the pricing construct for Azure Service Bus across the Standard and Premium tiers[[2]](#footnote-3):

|  |  |
| --- | --- |
| Standard Tier Messaging Operations | |
| Base charge 1 | **$0.0204**/hour |
| First 13M ops/month | Included |
| Next 87M ops (13-100M ops)/month | **$1.22** per million operations |
| Next 2,400M ops (100-2500M ops)/month | **$0.76** per million operations |
| Over 2,500M ops/month | **$0.31** per million operations |
| **Standard Tier Brokered Connections** |  |
| First 1K/month | Included |
| Next 99K (1K-100K)/month | **$0.05** per connection/month |
| Next 400K (100K-500K)/month | **$0.04** per connection/month |
| Over 500K/month | **$0.03** per connection/month |

Table 2: Pricing construct for Service Bus Standard tier

|  |  |
| --- | --- |
| Premium Tier Messaging Operations |  |
| Hourly | **$1.407**/hour/Messaging Unit |
| Premium Tier Brokered Connections |  |
| Brokered connections are not charged in the premium tier | |

Table 3: Pricing construct for Service Bus Premium tier

# 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

### Service Bus Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Evaluate Premium tier benefits of Azure Service Bus. | Yes | Yes | IaC | At deployment |
| **R2** | Connect to Service Bus with the AMQP protocol and use Service Endpoints or Private Endpoints when possible. | Yes | Yes | IaC  Operational | At deployment  Operational – during application deployment |
| **R3** | Implement geo-replication on the sender and receiver side to protect against outages and disasters. | Yes | No | Governance | Operational - |
| **R4** | Configure Geo-Disaster. | Yes | Yes | IaC | At deployment |
| **R5** | If you need mission-critical messaging with queues and topics, Service Bus Premium is recommended with Geo-Disaster Recovery. | Yes | Yes | IaC | At deployment |
| **R6** | Configure Zone Redundancy in the Service Bus namespace (only available with Premium tier). | No | No | N/A | N/A |
| **R7** | Implement high availability for the Service Bus namespace. | Yes | No | Governance | At deployment |
| **R8** | Ensure related messages are delivered in guaranteed order. | Yes | No | Governance | Operational – during application design |
| **R9** | Evaluate different JMS features through the JMS API. | Yes | No | Governance | Operational – application team configuration |
| **R10** | Implement resilience for transient fault handling when sending or receiving messages. | Yes | No | Governance | Operational – during application design and deployment |
| **R11** | Implement auto-scaling of messaging units, to ensure that you have enough resources available for your workloads. | Yes | Yes | IaC | At deployment |

Table 4: 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

### Service Bus Cost Optimisation Checklist

There is no guidance for Service Bus under the Cost Optimisation pillar.

## 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

### Service Bus Operational Excellence Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **OE1** | Establish a process to actively monitor the dead-letter queue (dlq) messages. | Yes | No | Governance | Operational – at deployment |
| **OE2** | Analyze the differences between Azure Storage Queues and Azure Service Bus Queues. | Yes | No | Governance | Operational – review before deployment |

Table 5: WAF Operational Excellence checklist summary

## 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

### Service Bus Performance Efficiency Checklist

There is no guidance for Service Bus 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
* NS-2: Secure cloud services with network controls
* 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
* LT-4: Enable logging for security investigation

# Architecture Summary

## Resource Overview

Data is transferred between applications and services using messages, which are a container with metadata. The data can be of any kind, inclusive of common formats such as JSON, XML, and Plain Text. Messages are sent to and received from queues, which are storage holds until the receiver can process the incoming information. Azure Service Bus is a message broker with message queues and publish-subscribe topics. It can be used to decouple applications and services with the additional following benefits[[7]](#footnote-8):

* Load -balancing work across workers
* Data routing and control across application and service boundaries
* Reliable coordination of transactional work

The following shows the high-level operation of Service Bus:

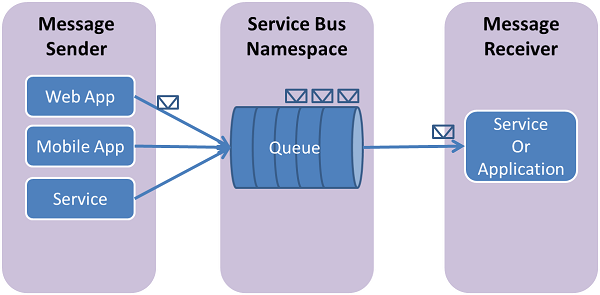


Figure : Service Bus flow diagram[[8]](#footnote-9)

## RBAC

The following roles can be assigned for Service Bus[[9]](#footnote-10):

|  |  |
| --- | --- |
| Role Name | Description |
| Azure Service Bus Data Owner | Allows for full access to Azure Service Bus resources. |
| Azure Service Bus Data Receiver | Allows for receive access to Azure Service Bus resources. |
| Azure Service Bus Data Sender | Allows for send access to Azure Service Bus resources. |

Table 6: 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 Service Bus 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:** Table 4 – [R1, R5](#_Service_Bus_Reliability)

**Design Decision**: the Premium tier will be used for Production workloads and can be used for Non-Production workloads as well if private connectivity is required on all tiers.

**Design Justification**: Geo-Disaster Recovery is only available in the Premium tier of Azure Service Bus. The Standard SKU can be used for Non-Production noting that this SKU does not support private endpoints. If preferred the Premium tier can be used for all deployments.

### Network Connectivity

**Design Reference:** Microsoft Security Benchmark [NS-1,NS-2](#_Overview), Table 4 – [R2](#_Service_Bus_Reliability)

**Design Decision:** The Virtual Network deployment with Private Endpoints will be used for Service Bus.

**Design Justification:** The most secure form of connectivity is through deploying the service in a private virtual network with a private endpoint. Note that to use this the Premium tier must be selected.

### Authentication

**Design Reference:** Microsoft Security Benchmark [IM-1, IM-3](#_Overview)

**Design Decision:** Managed Identities will be used for authentication instead of Service Principals. Local authentication will be disabled on the service and Microsoft Entra ID will be used for user authentication.

**Design Justification:** For applications, Managed Identities are preferred to Service Principals as Microsoft manage the underlying key rotations for Managed Identities and reduces the risk that users are hard-coding credentials required for Service Principals.

For user authentication, Azure AD (Microsoft Entra ID) authentication will be used and local authentication will be disabled. Again this uses the centralised identity system with MFA, and removes the option for users to keep Shared Access Signature keys hard-coded which are more easily compromised.

### Encryption

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

**Design Decision:** Minimum TLS will be set to 1.2.

**Design Justification:** Data at rest is automatically enabled by the service so no further action is required. For Data In Transit, the Minimum TLS will be set to 1.2 to prevent less secure protocols from being used to transmit messages.

### Geo-redundancy and High Availability

**Design Reference:** Table 4 - [R3, R4, R5](#_Service_Bus_Reliability), R7

**Design Decision:** Geo-redundancy will be enabled for Production workloads. This by default also creates High Availability.

**Design Justification:** Geo-redundancy and High Availability will protect applications leveraging the messaging service through Service Bus from outages. This configuration does require a second Premium tier service bus in the secondary region. This is not required for Non-Production workloads.

### Autoscaling

**Design Reference:** Table 4 – [R11](#_Service_Bus_Reliability)

**Design Decision:** Autoscaling will be enabled for Production workloads.

**Design Justification:** Autoscaling allows applications to continue to run even if a certain threshold of the Service Bus has been reached. It is recommended to set a metric-based threshold, such as CPU, to trigger scale out. CPU of 80% will be set as a condition for scale out, and more can be added depending on application requirements.

### Logging

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

**Design Decision:** Logging will be enabled, and logs sent to the central log analytics workspace for that region.

**Design Justification:** Logging of resource diagnostics and metrics is required for troubleshooting should any issues occur with the service and is a security mandate to maintain specific logs.

# Azure Policies

There are no Azure Policies required for this service.

# Configuration Templates

## Primary Region Production Service Bus Namespace

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sbns-prd-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Location** | Australia Southeast |
| **Pricing Tier** | Premium |
| **Minimum TLS** | Version 1.2 |
| **Local Authentication** | Disabled |
| **Partitioning** | Enabled/Disabled |
| **Messaging units** | 1/2/4/8/16 |
| **Network Connectivity** | Private Access |
| **Geo-redundancy** | Enabled |
| **Secondary Namespace** | sbns-dr-auea-[appname]-01 |
| ***Private Endpoint Settings*** |  |
| **Name** | pep-sbns-prd-ause-[appname]-01 |
| **Virtual Network** | vnet-prd-ause-[appname]-01 |
| **Subnet** | snet-prd-ause-[appname]-[workload]-01 |
| **Private DNS Zone** | privatelink.servicebus.windows.net |
| ***Diagnostic Settings*** |  |
| **Logs to capture** | allLogs, AllMetrics |
| **Log Analytics Workspace** | log-prd-ause-mgmt-01 |

## Secondary Region Production Service Bus Namespace

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sbns-dr-auea-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Location** | Australia East |
| **Pricing Tier** | Premium |
| **Minimum TLS** | Version 1.2 |
| **Local Authentication** | Disabled |
| **Partitioning** | Enabled/Disabled |
| **Messaging units** | 1/2/4/8/16 |
| **Network Connectivity** | Private Access |
| **Geo-redundancy** | Enabled |
| **Secondary Namespace** | sbns-prd-ause-[appname]-01 |
| ***Private Endpoint Settings*** |  |
| **Name** | pep-sbns-dr-auea-[appname]-01 |
| **Virtual Network** | vnet-dr-auea-[appname]-01 |
| **Subnet** | snet-dr-auea-[appname]-[workload]-01 |
| **Private DNS Zone** | privatelink.servicebus.windows.net |
| ***Diagnostic Settings*** |  |
| **Logs to capture** | allLogs, AllMetrics |
| **Log Analytics Workspace** | log-prd-auea-mgmt-01 |

## Primary Region Non-Production Service Bus Namespace

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| **Name** | sbns-[env]-ause-[appname]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Location** | Australia Southeast |
| **Pricing Tier** | Premium |
| **Minimum TLS** | Version 1.2 |
| **Local Authentication** | Disabled |
| **Partitioning** | Enabled/Disabled |
| **Messaging units** | 1/2/4/8/16 |
| **Network Connectivity** | Private Access |
| **Geo-redundancy** | Disabled |
| ***Private Endpoint Settings*** |  |
| **Name** | pep-sbns-[env]-ause-[appname]-01 |
| **Virtual Network** | vnet-[env]-ause-[appname]-01 |
| **Subnet** | snet-[env]-ause-[appname]-[workload]-01 |
| **Private DNS Zone** | privatelink.servicebus.windows.net |
| ***Diagnostic Settings*** |  |
| **Logs to capture** | allLogs, AllMetrics |
| **Log Analytics Workspace** | log-prd-ause-mgmt-01 |

# 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/service-bus/ [↑](#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/service-bus-messaging/service-bus-messaging-overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/service-bus-messaging/service-bus-quickstart-cli [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-10)