**CORE SERVICE DESIGN:**

**Event Hub**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Event Hub Core Service Design |
| **File Name** | Ambulance Victoria – Event Hub Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 21/12/2023 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 21/12/2023 |

Table of Contents

[1. Overview 5](#_Toc154066036)

[1.1 Purpose and Audience 5](#_Toc154066037)

[1.2 Scope and Key Deliverables 5](#_Toc154066038)

[1.3 Glossary and Definitions 6](#_Toc154066039)

[2. Executive Summary 7](#_Toc154066040)

[3. Resource Cost 8](#_Toc154066041)

[4. WAF and Security Control Alignment 8](#_Toc154066042)

[4.1 Reliability 9](#_Toc154066043)

[4.1.1 Overview 9](#_Toc154066044)

[4.1.2 Event Hub Reliability Checklist 9](#_Toc154066045)

[4.2 Cost Optimisation 10](#_Toc154066046)

[4.2.1 Overview 10](#_Toc154066047)

[4.2.2 Event Hub Cost Optimisation Checklist 10](#_Toc154066048)

[4.3 Operational Excellence 11](#_Toc154066049)

[4.3.1 Overview 11](#_Toc154066050)

[4.3.2 Event Hub Operational Excellence Checklist 11](#_Toc154066051)

[4.4 Performance Efficiency 11](#_Toc154066052)

[4.4.1 Overview 11](#_Toc154066053)

[4.4.2 Event Hub Performance Efficiency Checklist 11](#_Toc154066054)

[4.5 Security 12](#_Toc154066055)

[4.5.1 Overview 12](#_Toc154066056)

[5. Architecture Summary 13](#_Toc154066057)

[5.1 Resource Overview 13](#_Toc154066058)

[5.2 RBAC 14](#_Toc154066059)

[5.3 Solution Diagram 14](#_Toc154066060)

[5.4 Design Decisions and Justifications 15](#_Toc154066061)

[5.4.1 SKU Selection 15](#_Toc154066062)

[5.4.2 Event Partitions 15](#_Toc154066063)

[5.4.3 Geo-Disaster Recovery 16](#_Toc154066064)

[5.4.4 Capture Feature 17](#_Toc154066065)

[5.4.5 Network Security and Connectivity 17](#_Toc154066066)

[5.4.6 Access and Authentication 18](#_Toc154066067)

[5.4.7 Encryption 18](#_Toc154066068)

[5.4.8 Logging and Monitoring 18](#_Toc154066069)

[6. Azure Policies 19](#_Toc154066070)

[7. Configuration Templates 19](#_Toc154066071)

[7.1 Primary Platinum Event Hub 19](#_Toc154066072)

[7.2 DR Platinum Event Hub 20](#_Toc154066073)

[7.3 Primary Gold and Silver Event Hub 21](#_Toc154066074)

[7.4 Primary Bronze Event Hub 22](#_Toc154066075)

[8. Acceptance 24](#_Toc154066076)

# Overview

This document covers the baseline design for the Event Hub 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 Event Hub 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 an Event Hub.

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 Event Hub 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 Event Hub 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. Operational Excellence and Reliability had identical recommendations so only the Reliability checklist has been populated to remove duplications.

For this service the main baseline configurations include:

* Connectivity will not allow public access.
* The Standard SKU is recommended for all service tiers.
* Local authentication will be disabled.
* Managed Identity will be used for this service.

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

* Geo-Disaster Recovery will be enabled for Platinum only.
* The Platinum configuration will have a higher default value of Throughput Units and Partitions
* The Platinum configuration will have a longer retention time.

# Resource Cost

The pricing for Event Hub is as follows[[2]](#footnote-3):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SKU | Basic | Standard | Premium | Dedicated |
| Capacity | **$0.023**/hour per Throughput Unit | **$0.046**/hour per Throughput Unit | **$2.166**/hour per Processing Unit (PU) | **$12.913**/hour per [Capacity Unit (CU)](https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-faq#dedicated-clusters) |
| Ingress events | **$0.043** per million events | **$0.043** per million events | Included | Included |
| Capture | Not available | **$109.915**/month per Throughput Unit\*\*\* | Included | Included |
| Apache Kafka | Not available | Available | Available | Available |
| Schema Registry | Not available | Available | Available | Available |
| Max Retention Period | 1 day | 7 days | 90 days | 90 days |
| Storage Retention | 84 GB | 84 GB | 1 TB per PU | 10 TB per CU |
| Extended Retention | Not available | Not available | **$0.22**/GB/month (1 TB inc. per PU) | **$0.22**/GB/month (10 TB inc. per CU) |

Table 2: Pricing construct

# 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

### Event Hub Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | When using the SDK to send events to Event Hubs, ensure the exceptions thrown by the retry policy (EventHubsException or OperationCancelledException) are properly caught. | Yes | No | Governance | During Application Deployment |
| **R2** | In high-throughput scenarios, use batched events. | Yes | No | Governance | During Application Deployment |
| **R3** | Every consumer can read events from one to 32 partitions. | Yes | Yes | IaC | At deployment |
| **R4** | When developing new applications, use EventProcessorClient (.NET and Java) or EventHubConsumerClient (Python and JavaScript) as the client SDK. | N/A | N/A | N/A | This feature has been deprecated |
| **R5** | As part of your solution-wide availability and disaster recovery strategy, consider enabling the Event Hubs geo disaster-recovery option. | Yes | Yes | IaC | At deployment |
| **R6** | When a solution has a large number of independent event publishers, consider using Event Publishers for fine-grained access control. | Yes | No | Governance | During Application Deployment |
| **R7** | Don't publish events to a specific partition. | Yes | No | Governance | During Application Deployment |
| **R8** | When publishing events frequently, use the AMQP protocol when possible. | Yes | No | Governance | During Application Deployment |
| **R9** | The number of partitions reflect the degree of downstream parallelism you can achieve. | Yes | Yes | IaC | At deployment |
| **R10** | When using the Capture feature, carefully consider the configuration of the time window and file size, especially with low event volumes. | Yes | No | No | Not required – to be included by exception for a specific application requirement |

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

### Event Hub Cost Optimisation Checklist

There is no guidance for Cost Optimisation for the Event Hub service. Costs will be managed with appropriate SKU selection and configuration.

## 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

### Event Hub Operational Excellence Checklist

The guidance for Operational Excellence was identical to the Reliability guidance, so this section has not been filled in to remove duplication.

## 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

### Event Hub Performance Efficiency Checklist

There is no guidance for Performance Efficiency for the Event Hub service.

## 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 guidelines apply[[7]](#footnote-8):

* NS-1: Establish network segmentation boundaries
  + Private Network injection
  + Service Tags
* NS-2: Secure cloud services with network controls
  + Private Endpoints
* IM-1: Use centralized identity and authentication system
* IM-3: Manage application identities securely and automatically
* PA-1: Separate and limit highly privileged/administrative users
* PA-7: Follow just enough administration (least privilege) principle
* DP-3: Encrypt sensitive data in transit
* DP-4: Enable data at rest encryption by default
* LT-4: Enable logging for security investigation

There are no Department of Health controls above and beyond the Microsoft Security Benchmark for this service.

# Architecture Summary

## Resource Overview

Azure Event Hub is a data-streaming platform that can stream millions of events per second[[8]](#footnote-9). It can ingest from any source and send to any destination and includes inbuilt compatibilities such as with Apache Kafka. Event Hub is typically used as the ingestion layer of a streaming solution, and its applicability ranges from receiving and sending logs for security purposes, to being a small part of a complete data analytics architecture.

Event Hub has several SKU tiers which vary in capability as follows[[9]](#footnote-10):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Feature | Basic | Standard | Premium | Dedicated |
| Tenancy | Multi-tenant | Multi-tenant | Multi-tenant with resource isolation | Exclusive single tenant |
| Private link | N/A | Yes | Yes | Yes |
| Customer-managed key (Bring your own key) | N/A | N/A | Yes | Yes |
| Capture | N/A | Priced separately | Included | Included |
| Dynamic Partition scale out | N/A | N/A | Yes | Yes |
| Ingress events | Pay per million events | Pay per million events | Included | Included |
| Runtime audit logs | N/A | N/A | Yes | Yes |
| Availability Zone | Yes | Yes | Yes | Yes |
| Geo disaster | N/A | Yes | Yes | Yes |
| IP Firewall | N/A | Yes | Yes | Yes |

Table 4: Event Hub SKU tier feature comparison

## RBAC

The specific roles that can be applied for Azure Event Hub are as follows[[10]](#footnote-11) [[11]](#footnote-12):

|  |  |
| --- | --- |
| Role | Description |
| Azure Event Hubs Data owner | Use this role to give complete access to Event Hubs resources. |
| Azure Event Hubs Data sender | Use this role to give the send access to Event Hubs resources. |
| Azure Event Hubs Data receiver | Use this role to give the consuming/receiving access to Event Hubs resources. |
| Schema Registry Reader | Read and list Schema Registry groups and schemas. |
| Schema Registry Contributor | Read, write, and delete Schema Registry groups and schemas. |

Table 5: RBAC roles relevant for this core service

## Diagram that shows how Azure Event Hubs fits in an event streaming platform.Solution Diagram

Figure 1: Example Event Hub architecture in a data analytics architecture

## 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 Event Hub 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.

### SKU Selection

**Design Reference:** Cost Optimisation Section

**Design Decision**: The Basic and Premium SKUs will not be used. The Standard and Dedicated SKUs are recommended however the Dedicated SKU is not currently available in Australia Southeast. Hence, Standard will be used.

**Design Justification**: The Basic SKU does not include key security features such as Private Link and Geo-Disaster recovery. The Premium SKU is a multi-tenanted SKU which does not make sense to use for Ambulance Victoria’s single tenancy configuration. As such the SKUs will be limited to Standard. Dedicated is also recommended however is not currently available in Australia Southeast.

### Event Partitions

**Design Reference:** Table 2 – [R3, R9](#_Event_Hub_Reliability)

**Design Decision:** the full number (32) of partitions will not be automatically added. This number will be decided during the application and platform landing zone design processes. The baseline number of partitions is assumed to be 4 for larger expected levels of throughput, and 1 for smaller or single-purpose Event Hubs.

**Design Justification:** though partitions do not directly cost additional money, more partitions may mean that more Throughput Units are required, and these will have a financial implication. As such it is not recommended to use all 32 available slots.

**Design Details:** The formula to determine the number of partitions is related to the ingress of data, the number of events, and the throughput required. There are several principles that can be followed to determine the required number of partitions per deployment[[12]](#footnote-13):

* Use at least as many partitions as the value of your target throughput in megabytes.
* Use at least as many partitions as customers/receiver.

Alternatively, the maximum of target throughput divided by production through a single partition, or target throughput divided by consumption on a single partition can be used as shown in the following example12:

The ideal throughput is 2 MBps. For the formula, t is 2 MBps. A producer sends events at a rate of 1,000 events per second, making p 1 MBps. A consumer receives events at a rate of 500 events per second, setting c to 0.5 MBps.

max(t/p, t/c) = max(2/1, 2/0.5) = max(2, 4) = 4

Currently the largest number of partitions used for a single event hub in the Ambulance Victoria tenancy is 4 and this will be used as a baseline for deployments that are expected to have larger amounts of ingested data. For Event Hubs that are used for a single purpose, such as alerting for a specific application, a default value of 1 partition will be assumed.

### Geo-Disaster Recovery

**Design Reference:** Table 2 – R5

**Design Decision:** Geo-Disaster Recovery will be enabled for Event Hubs that are in use for Platinum services. All other Event Hubs may or may not have Geo-Disaster Recovery enabled depending on the application requirement and criticality.

**Design Justification:** It is a security requirement to ensure that all services that contain critical data are recoverable, and an operational requirement is that Platinum services are rapidly able to recover. For Event Hubs that are being used as Platinum deployments, or used to ingest critical data and workloads, these will have Geo-Disaster Recovery enabled.

**Design Details:** To enable Geo-Disaster Recovery a secondary Event Hub namespace will be required at deployment so that the entire configuration of the namespace is replicated to the secondary namespace[[13]](#footnote-14). The failover sequence is near instantaneous once initiated. Note that the replication does not replicate the event data, and this data is preserved in the primary hub and recoverable post-failover.

Given that Private Endpoints are the recommended network connectivity method, the Disaster recovery configuration for Event Hub will require both namespaces to have Private Connectivity enabled with each namespace having a Private Endpoint in both subnets in each region, as shown in the diagram below:

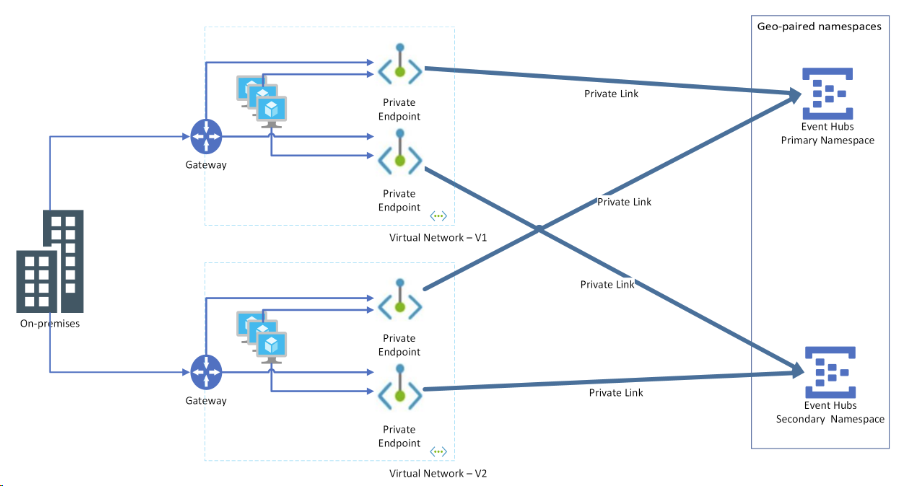


Figure 2: Event Hub namespace resilient configuration with Private Endpoints[[14]](#footnote-15)

### Capture Feature

**Design Reference:** Table 2 – [R10](#_Event_Hub_Reliability)

**Design Decision:** the Capture Feature will not be enabled by default.

**Design Justification:** At this stage there is no specific requirement for this feature as the current use-case for Event Hub is to forward logs to other locations that will store this information. At this stage, using the Capture Feature to store the events would be redundant, and would have cost implications for the storage required to use this. Should an application in future require this feature, likely as part of a larger data analytics deployment, this feature can be enabled but should be approved by the relevant forums.

### Network Security and Connectivity

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

**Design Decision:** Private Endpoints will be used for connectivity and Service Tags will be used in place of specific IP addresses for any required security rules.

**Design Justification:** It is a Security requirement to restrict network access as much as possible. The most secure connectivity method is Private Endpoints. Additionally, where security rules are required, Service Tags are preferred when allowing or denying access to Event Hubs as specific IPs may change over time for this service, but the Service Tags will be auto updated in the background by Microsoft so the service will not be disrupted.

### Access and Authentication

**Design Reference:** Microsoft Security Benchmark – [IM-2, IM-3](#_Overview)

**Design Decision:** Azure AD authentication will be used as the primary authentication method. Shared Access Signatures will only be used if Azure AD authentication is impossible.Additionally, Managed Identities will be used over service principals where possible.Local Authentication will be disabled.

**Design Justification:** Azure AD authentication is the preferred method as local username and passwords can be easily weaponised, whereas Azure AD Authentication will require additional authentication steps such as MFA.

Managed Identities are preferred to service principals as Azure automatically rotates credentials for Managed Identities in the background and this is completely managed by Microsoft. It also avoids hardcoding credentials in code or configuration files.

### Encryption

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

**Design Decision:** no action is required as the service supports data in transit and data at rest encryption by default. **T**he minimum TLS will be set to 1.2.

**Design Justification:** It is a security requirement that all data is encrypted at rest and in transit. This is a default configuration for Azure Event Hub. The only action required is to set the Minimum TLS version, which will be 1.2.

### Logging and Monitoring

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

**Design Decision:** audit and allMetrics will be sent to the central Log Analytics Workspace for that region. Most logs will be enabled by default, except for Runtime and Application Metrics logs.

**Design Justification: Runtime and Application metric logs are used** to monitor the data plane interactions of client applications. For the current use case these are not required as the Event Hub is intended to be used to forward logs, not analyse them. However, these can optionally be enabled should a specific application deployment require.

# Azure Policies

There are no additional Azure Policies required for Event Hubs.

# Configuration Templates

## Primary Platinum Event Hub

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ [Subscription Name] |
| Namespace Name | ehns-prd-ause-[appname]-[workload]-01 |
| Location | Australia Southeast |
| Pricing Tier | Standard |
| Throughput Units | 2 [up to 40 allowed if required for workload] |
| Auto-Inflate enable | Yes |
| Maximum Throughput Units | 4 [up to 40 allowed if required for workload] |
| Minimum TLS | 1.2 |
| Local Authentication | Disabled |
| Geo-Recovery | Enabled |
| Identity | System-Assigned managed identity enabled |
| ***Event Hubs Details*** |  |
| Name | eh-prd-ause-[appname]-[workload]-01 |
| Partition Count | 4 [1 to 32 can be used depending on workload requirements] |
| Cleanup Policy | Delete |
| Retention time (hrs) | 24 |
| Capture | Off [can be enabled if required by workload] |
| Network Connectivity | Private Access |
| ***Private Endpoint Details*** |  |
| Private Endpoint | pe-ehns-prd-ause-[appname]-[workload]-01 |
| Target Sub-resource | Namespace |
| Virtual Network | vnet-prd-ause-[appname]-01 |
| Subnet | Sn-prd-ause-[appname]-[workload]-01 |
| Integrate with Private DNS | Yes |
| Private DNS Zone | privatelink.servicebus.windows.net |
| ***Diagnostic Setting Details*** |  |
| Log Analytics Workspace | law-prd-ause-mgmt-01 |
| Logs | Audit  AllMetrics  Archive Logs  Operational Logs  Auto Scale Logs  VNet/IP Filtering Connection Logs |

## DR Platinum Event Hub

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ [Subscription Name] |
| Namespace Name | ehns-dr-auea-[appname]-[workload]-01 |
| Location | Australia East |
| Pricing Tier | Standard |
| Throughput Units | 2 [up to 40 allowed if required for workload] |
| Auto-Inflate enable | Yes |
| Maximum Throughput Units | 4 [up to 40 allowed if required for workload] |
| Minimum TLS | 1.2 |
| Local Authentication | Disabled |
| Geo-Recovery | Enabled |
| Identity | System-Assigned managed identity enabled |
| ***Event Hubs Details*** |  |
| Name | eh-dr-auea-[appname]-[workload]-01 |
| Partition Count | 4 [1 to 32 can be used depending on workload requirements] |
| Cleanup Policy | Delete |
| Retention time (hrs) | 24 |
| Capture | Off [can be enabled if required by workload] |
| Network Connectivity | Private Access |
| ***Private Endpoint Details*** |  |
| Private Endpoint | pe-ehns-dr-auea-[appname]-[workload]-01 |
| Target Sub-resource | Namespace |
| Virtual Network | vnet-dr-auea-[appname]-01 |
| Subnet | sn-dr-auea-[appname]-[workload]-01 |
| Integrate with Private DNS | Yes |
| Private DNS Zone | privatelink.servicebus.windows.net |
| ***Diagnostic Setting Details*** |  |
| Log Analytics Workspace | law-prd-auea-mgmt-01 |
| Logs | Audit  AllMetrics  Archive Logs  Operational Logs  Auto Scale Logs  VNet/IP Filtering Connection Logs |

## Primary Gold and Silver Event Hub

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ [Subscription Name] |
| Namespace Name | ehns-[env]-ause-[appname]-[workload]-01 |
| Location | Australia Southeast |
| Pricing Tier | Standard |
| Throughput Units | 1 [up to 40 allowed if required for workload] |
| Auto-Inflate enable | Yes |
| Maximum Throughput Units | 2 [up to 40 allowed if required for workload] |
| Minimum TLS | 1.2 |
| Local Authentication | Disabled |
| Geo-Recovery | Disabled |
| Identity | System-Assigned managed identity enabled |
| ***Event Hubs Details*** |  |
| Name | eh-[env]-ause-[appname]-[workload]-01 |
| Partition Count | 2 [1 to 32 can be used depending on workload requirements] |
| Cleanup Policy | Delete |
| Retention time (hrs) | 8 |
| Capture | Off [can be enabled if required by workload] |
| Network Connectivity | Private Access |
| ***Private Endpoint Details*** |  |
| Private Endpoint | pe-ehns-[env]-ause-[appname]-[workload]-01 |
| Target Sub-resource | Namespace |
| Virtual Network | vnet-[env]-ause-[appname]-01 |
| Subnet | sn-[env]-ause-[appname]-[workload]-01 |
| Integrate with Private DNS | Yes |
| Private DNS Zone | privatelink.servicebus.windows.net |
| ***Diagnostic Setting Details*** |  |
| Log Analytics Workspace | law-prd-ause-mgmt-01 |
| Logs | Audit  AllMetrics  Archive Logs  Operational Logs  Auto Scale Logs  VNet/IP Filtering Connection Logs |

## Primary Bronze Event Hub

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ [Subscription Name] |
| Namespace Name | ehns-[env]-ause-[appname]-[workload]-01 |
| Location | Australia Southeast |
| Pricing Tier | Standard |
| Throughput Units | 1 [up to 40 allowed if required for workload] |
| Auto-Inflate enable | No |
| Minimum TLS | 1.2 |
| Local Authentication | Disabled |
| Geo-Recovery | Disabled |
| Identity | System-Assigned managed identity enabled |
| ***Event Hubs Details*** |  |
| Name | eh-[env]-ause-[appname]-[workload]-01 |
| Partition Count | 2 [1 to 32 can be used depending on workload requirements] |
| Cleanup Policy | Delete |
| Retention time (hrs) | 1 |
| Capture | Off [can be enabled if required by workload] |
| Network Connectivity | Private Access |
| ***Private Endpoint Details*** |  |
| Private Endpoint | pe-ehns-[env]-ause-[appname]-[workload]-01 |
| Target Sub-resource | namespace |
| Virtual Network | vnet-[env]-ause-[appname]-01 |
| Subnet | sn-[env]-ause-[appname]-[workload]-01 |
| Integrate with Private DNS | Yes |
| Private DNS Zone | privatelink.servicebus.windows.net |
| ***Diagnostic Setting Details*** |  |
| Log Analytics Workspace | law-prd-ause-mgmt-01 |
| Logs | Audit  AllMetrics  Archive Logs  Operational Logs  Auto Scale Logs  VNet/IP Filtering Connection Logs |

# 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/event-hubs/ [↑](#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/security/benchmark/azure/baselines/event-hubs-security-baseline [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-about [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/event-hubs/compare-tiers [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/event-hubs/authorize-access-azure-active-directory [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/azure/event-hubs/schema-registry-concepts#azure-role-based-access-control [↑](#footnote-ref-12)
12. https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/event-hubs/partitioning-in-event-hubs-and-kafka [↑](#footnote-ref-13)
13. https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-geo-dr?tabs=portal [↑](#footnote-ref-14)
14. https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-geo-dr?tabs=portal [↑](#footnote-ref-15)