**CORE SERVICE DESIGN:**

**Private Endpoint & Azure Private DNS**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Private Endpoint & Azure Private DNS Core Service Design |
| **File Name** | Ambulance Victoria – Private Endpoint & Azure Private DNS Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 18/01/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 18/01/2024 |
| 2.0 | Updates | Minor Feedback | 7, 14, 17 | 24/01/2024 |

Table of Contents

[1. Overview 5](#_Toc156483692)

[1.1 Purpose and Audience 5](#_Toc156483693)

[1.2 Scope and Key Deliverables 5](#_Toc156483694)

[1.3 Glossary and Definitions 6](#_Toc156483695)

[2. Executive Summary 7](#_Toc156483696)

[3. Resource Cost 8](#_Toc156483697)

[4. WAF and Security Control Alignment 8](#_Toc156483698)

[4.1 Reliability 9](#_Toc156483699)

[4.1.1 Overview 9](#_Toc156483700)

[4.1.2 Private Endpoint & Azure Private DNS Reliability Checklist 9](#_Toc156483701)

[4.2 Cost Optimisation 10](#_Toc156483702)

[4.2.1 Overview 10](#_Toc156483703)

[4.2.2 Private Endpoint & Azure Private DNS Cost Optimisation Checklist 10](#_Toc156483704)

[4.3 Operational Excellence 10](#_Toc156483705)

[4.3.1 Overview 10](#_Toc156483706)

[4.3.2 Private Endpoint & Azure Private DNS Operational Excellence Checklist 10](#_Toc156483707)

[4.4 Performance Efficiency 11](#_Toc156483708)

[4.4.1 Overview 11](#_Toc156483709)

[4.4.2 Private Endpoint & Azure Private DNS Performance Efficiency Checklist 11](#_Toc156483710)

[4.5 Security 11](#_Toc156483711)

[4.5.1 Overview 11](#_Toc156483712)

[5. Architecture Summary 12](#_Toc156483713)

[5.1 Resource Overview 12](#_Toc156483714)

[5.2 Resource Centralisation 12](#_Toc156483715)

[5.3 RBAC 13](#_Toc156483716)

[5.4 Solution Diagram 13](#_Toc156483717)

[5.5 Design Decisions and Justifications 14](#_Toc156483718)

[5.5.1 Private Endpoint Use 14](#_Toc156483719)

[5.5.2 Private Endpoint Policies 14](#_Toc156483720)

[5.5.3 Private DNS 14](#_Toc156483721)

[5.5.4 Logging 15](#_Toc156483722)

[6. Azure Policies 15](#_Toc156483723)

[7. Configuration Templates 16](#_Toc156483724)

[7.1 Configuration Templates 16](#_Toc156483725)

[7.1.1 Primary Region Private Endpoint 16](#_Toc156483726)

[7.1.2 Secondary Region Private Endpoint 16](#_Toc156483727)

[7.1.3 Private DNS Zones 16](#_Toc156483728)

[8. Acceptance 17](#_Toc156483729)

# Overview

This document covers the baseline design for the Private Endpoint & Azure Private DNS 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 Private Endpoint & Azure Private DNS 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 Private Endpoint & Azure Private DNS.

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 Private Endpoint & Azure Private DNS 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. |
| **PE** | Private Endpoint |
| **DNS** | Domain Name Services |
| **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 Private Endpoint & Azure Private DNS 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 applicable for Azure Private Endpoints and Private DNS Zones.

Azure Private Endpoints boots security and performance by establishing a private link to Azure services within a virtual network. This ensures resource isolation, meeting regulatory requirements and data residency standards. When combined with Private DNS Zones, an extra layer of isolation from external DNS services is achieved, preventing inadvertent exposure of internal resources through private name resolution.

By keeping data confined within the Azure network, Private Endpoints lower the risk of internet threats, providing a more secure and efficient means of connecting to Azure services while upholding compliance and optimizing performance.

For this service the main baseline configurations include:

* The Private Endpoint resources are to reside in the spoke closest to the application resources that require access to that specific service.
* The Private Endpoint must be connected to a Private DNS zone, which is in the AV ALZ Connectivity subscription.
* An A-record must be created in the related Private DNS zone in the hub for each Private Endpoint created[[2]](#footnote-3).

There are on differences between Platinum, Gold, Silver, or Bronze deployments for Private Endpoint. Due to the nature of the service, it is inherently Platinum as they support connectivity and networking.

# Resource Cost

Private Endpoints come with additional costs compared to accessing Azure services freely over a virtual network. These costs include the Private Endpoint itself and data transfer expenses, which vary based on the endpoint's region and the amount of data transferred. Despite the added costs, using Private Endpoints can potentially lower expenses by minimizing data transfer over the public internet, resulting in reduced egress charges and improved network performance. The following table shows the pricing construct for Private Endpoints[[3]](#footnote-4):

|  |  |
| --- | --- |
| Cost Item | Cost |
| Private Link Service | No charge for private link service |
| Private Endpoint | $0.016 per hour |
| Inbound Data Processed | 0-1 PB - $0.0151 per GB  1-5 PB - $0.0091 per GB  5+ PB - $0.0061 per GB |
| Outbound Data Processed | 0-1 PB - $0.0151 per GB  1-5 PB - $0.0091 per GB  5+ PB - $0.0061 per GB |

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[[4]](#footnote-5). 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

### Private Endpoint & Azure Private DNS Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Use Private Link, where available, for shared Azure PaaS services. Private Link is generally available for several services and is in public preview for numerous ones. | Yes | Yes | IaC | At deployment |
| **R2** | Use either virtual network injection for dedicated Azure services or Azure Private Link for available shared Azure services. To access Azure PaaS services from on-premises when virtual network injection or Private Link isn't available, use ExpressRoute with Microsoft peering. This method avoids transiting over the public internet. | Yes | No | N/A | Already in place |
| **R3** | Use virtual network service endpoints to secure access to Azure PaaS services from within your virtual network. Use virtual network service endpoints only when Private Link isn't available and there are no concerns with unauthorized movement of data. | Yes | Yes | IaC | At deployment |
| **R4** | Service Endpoints don't allow a PaaS service to be accessed from on-premises networks. Private Endpoints do. | Yes | Yes | IaC | At deployment |

Table 3: WAF Reliability checklist summary

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[5]](#footnote-6). 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

### Private Endpoint & Azure Private DNS Cost Optimisation Checklist

There is no guidance for cost optimisation for Private Endpoints or Private DNS. Azure Private Link is a free service.

## 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

### Private Endpoint & Azure Private DNS Operational Excellence Checklist

There is no guidance for Operational Excellence for Private Endpoint or Private DNS.

## 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[[6]](#footnote-7). This covers capacity and scalability:

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

### Private Endpoint & Azure Private DNS Performance Efficiency Checklist

There is no guidance for Performance Efficiency for Private Endpoint or Private DNS.

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

* 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:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud services with network controls
* LT-1: Enable threat detection capabilities
* LT-4: Enable logging for security investigation

There are no Department of Health controls above and beyond the Microsoft Benchmark.

# Architecture Summary

## Resource Overview

Azure offers several services that are related to Private Connectivity:

* Private Endpoint
* Private Link
* Private DNS

Azure Private Endpoint (PE) is a Network Interface that enables you to connect securely to Azure services[[8]](#footnote-9). This interface uses a private IP address from an existing Azure Virtual Network. Deploying a PE brings the service into your virtual network.

Private Link is a service that allows you to access PaaS services through a Private Endpoint in your own virtual network without exposing network traffic to the public internet[[9]](#footnote-10). A Private Link service can have many Private Endpoints pointing to it, but a Private Endpoint can only be attached to a single Private Link. A Private link is not always required. Typically, this is to privately render a service, as opposed to Private Endpoint which is typically used to connect to a service and is the more likely use case. In some cases, a service may have a pre-defined Private Link Scope required, such as Azure Arc.

Finally, to ensure that Private Endpoints can correctly resolve names against their Private IPs, a Private DNS zone is required for each service with some configuration also required in the On-Prem DNS to enable the use of custom DNS when Azure DNS is not being used.

## Resource Centralisation

For a hub-and-spoke architecture it is recommended to have the Private DNS zones centralised in the same location as the Hub network[[10]](#footnote-11). This centralised model is driven by cross-premises DNS name resolution, and RBAC control.

For Ambulance Victoria a resource group will host all the Private DNS zones, and for every new Private Endpoint deployment there will be a requirement to update the central Private DNS zone with an A record for the new Private Endpoint. This configuration is detailed in Figure 1 in the following section.

## RBAC

For this resource, the specific roles that can be applied are as follows:

|  |  |
| --- | --- |
| Role Name | Description |
| Network Contributor | Lets you manage networks, but not access to them. |

Table 7: RBAC roles relevant for this core service

## Solution Diagram



Figure 1: Private DNS and Private Endpoint Configuration (Including AZ 2 DCs)

## 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 Private Endpoint & Azure Private DNS 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.

### Private Endpoint Use and Deployment

**Design Reference:** Table 2 – [R1, R3, R4](#_Private_Endpoint_&)

**Design Decision**: Private Endpoints will be used to access services where available. If not available or possible for a specific deployment, Service Endpoints will be used. Public Access will not be allowed. Private Endpoints will be deployed in each spoke closest to the application that requires their use.

**Design Justification:** Private access to Azure resources is the most secure form of access to Azure services. It is a security requirement to use private connectivity wherever possible. If for any reason this is not available for a particular service, then Service Endpoints will be used. Public Access will not be allowed by default on any resource, and any applications that require access through the public Internet will need to either leverage existing constructs, such as Perimeter Services, or have a secure entry point such as an Azure Application Gateway.

Additionally, to support the segmentation strategy that Ambulance Victoria have, Private Endpoints will be deployed in spokes closest to the resources of the application using them. At this stage, each application has different requirements and will use different deployments of each service.

### Private Endpoint Policies

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

**Design Decision:** private endpoints policies will be left disabled by default in subnets that host a Private Endpoint unless specifically required for an application.

**Design Justification:** private endpoint policies can add more granular routing and management for private endpoints. There is no specific requirement for them to be enabled so they will be assumed to be disabled by default unless specifically required by the application in question.

### Private DNS

**Design Reference:** N/A

**Design Decision:** Private DNS Zones will be used for each Private Endpoint service deployed and will be used in conjunction with Custom DNS.

**Design Justification:** In order for the deployed Private Endpoints to have name resolution with the custom DNS currently in place, Private DNS zones are required to be created for each service. They will be created centrally in the Connectivity subscription, and will have a Vnet link to the subnet that hosts the DNS servers. Each time a new Private Endpoint is created for that service, if the Private DNS zone already exists, then an A record will need to be created in the central DNS zone.

For each Private DNS Zone a conditional forwarder is required on the DNS server.

### Logging

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

**Design Decision:** Resource logging is not available for the Private Endpoint or Private DNS zone resources themselves so cannot be enabled directly. NSG Flow Logs and Network Watcher resources with Azure Network Monitor will be used to manage logs for network connectivity.

**Design Justification:** There is currently no option to enable logging on Private Endpoint or Private DNS resources.

# Azure Policies

There are no Azure Policies required for Private Endpoints or Azure Private DNS.

# Configuration Templates

## Configuration Templates

### Primary Region Private Endpoint

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia Southeast |
| Virtual Network | vnet-[env]-ause-[appname]-01 |
| Associated Subnet | sn-[env]-ause-[appname]-[workload]-01 |
| Name | pe-[env]-ause-<appname>-<workload>-01 |
| NIC Name | nic-[env]-ause-[appname]-[workload]-01 |
| Resource Type | Select resource e.g. Key Vault, Storage |
| Resource | Select the specific resource |
| DNS Zone | privatelink.[zone required] |

### Secondary Region Private Endpoint

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia Southeast |
| Virtual Network | vnet-[env]-ause-[appname]-01 |
| Associated Subnet | sn-[env]-ause-[appname]-[workload]-01 |
| Name | pe-[env]-ause-<appname>-<workload>-01 |
| NIC Name | nic-[env]-ause-[appname]-[workload]-01 |
| Resource Type | Select resource e.g. Key Vault, Storage |
| Resource | Select the specific resource |
| DNS Zone | privatelink.[zone required] |

### Private DNS Zones

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ Connectivity |
| Region | Australia Southeast |
| Resource Group | rg-prd-ause-connectivity-privatedns-01 |
| Name | Default Private DNS zone name: e.g. privatelink.service.net |
| Vnet Links | dnsvnl-to-vnet-prd-syd-shd-01 (AZ 2 Sydney)  dnsvnl-to-vnet-prd-mel-shd-01 (AZ 2 Melbourne)  dnsvnl-to-vnet-prd-auea-iden-01 (AZ 3 Sydney)  dnsvnl-to-vnet-prd-ause-iden-01 (AZ 3 Melbourne) |

*Note that the vnet links above to AZ 2 will eventually be terminated when all Virtual Networks point to the Domain Controllers in AZ 3 for the DNS service.*

# Appendix

## Associated Links

Note that the following Confluence documentation is heavily linked to this design document:

<https://ambvic.atlassian.net/wiki/spaces/Infr/pages/2921889793/Private+Endpoint+DNS+Integration>

[https://ambvic.atlassian.net/wiki/spaces/Infr/pages/2927394829/DNS+DHCP+Infrastructure](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fambvic.atlassian.net%2Fwiki%2Fspaces%2FInfr%2Fpages%2F2927394829%2FDNS%2BDHCP%2BInfrastructure&data=05%7C02%7Cven1tddn%40AMBULANCE.VIC.GOV.AU%7C1edfe60bc1ce4f54625808dc1b9d09f2%7C86b0e251f8cb4d7aabd236a8896457e7%7C0%7C0%7C638415608485384177%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=T0%2BZjinsSdiC%2Bf9Bl%2F5F5Yk9UllqQbbeGf%2BwX0YC5gU%3D&reserved=0)

# 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://learn.microsoft.com/en-us/azure/private-link/private-endpoint-dns [↑](#footnote-ref-3)
3. https://azure.microsoft.com/en-us/pricing/details/private-link/ [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/private-link/private-link-faq [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/private-link/private-link-service-overview [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/private-link-and-dns-integration-at-scale [↑](#footnote-ref-11)