**CORE SERVICE DESIGN:**

**Traffic Manager**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Traffic Manager Core Service Design |
| **File Name** | Ambulance Victoria – Traffic Manager Core Service Designv2.1.docx |
| **Version** | 2.1 |
| **Status** | Updated |
| **Release Date** | 08/01/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Ron Deivanayagam | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 11/12/2023 |
| 2.0 | Minor Updates | Include Public DNS Zone | 7,8,13,16,17 | 20/12/2023 |
| 2.1 | Minor Updates | Minor updates | 13, 14 | 08/01/2024 |

Table of Contents

[1. Overview 5](#_Toc153961355)

[1.1 Purpose and Audience 5](#_Toc153961356)

[1.2 Scope and Key Deliverables 5](#_Toc153961357)

[1.3 Glossary and Definitions 6](#_Toc153961358)

[2. Executive Summary 7](#_Toc153961359)

[3. Resource Cost 8](#_Toc153961360)

[4. WAF and Security Control Alignment 9](#_Toc153961361)

[4.1 Reliability 9](#_Toc153961362)

[4.1.1 Overview 9](#_Toc153961363)

[4.1.2 Traffic Manager Reliability Checklist 9](#_Toc153961364)

[4.2 Cost Optimisation 10](#_Toc153961365)

[4.2.1 Overview 10](#_Toc153961366)

[4.2.2 Traffic Manager Cost Optimisation Checklist 10](#_Toc153961367)

[4.3 Operational Excellence 11](#_Toc153961368)

[4.3.1 Overview 11](#_Toc153961369)

[4.3.2 Traffic Manager Operational Excellence Checklist 11](#_Toc153961370)

[4.4 Performance Efficiency 11](#_Toc153961371)

[4.4.1 Overview 11](#_Toc153961372)

[4.4.2 Traffic Manager Performance Efficiency Checklist 11](#_Toc153961373)

[4.5 Security 12](#_Toc153961374)

[4.5.1 Overview 12](#_Toc153961375)

[4.5.2 Traffic Manager Security Checklist 12](#_Toc153961376)

[5. Architecture Summary 13](#_Toc153961377)

[5.1 Resource Overview 13](#_Toc153961378)

[5.2 Configuring Public DNS Zones 13](#_Toc153961379)

[5.2.1 Routing Methods Overview 13](#_Toc153961380)

[5.3 RBAC 14](#_Toc153961381)

[5.4 Design Decisions and Justifications 14](#_Toc153961382)

[5.4.1 DNS TTL 14](#_Toc153961383)

[5.4.2 Custom pages 14](#_Toc153961384)

[5.4.3 Routing Methods 15](#_Toc153961385)

[5.4.4 Nested Profiles 15](#_Toc153961386)

[5.4.5 Diagnostics 15](#_Toc153961387)

[5.4.6 Alerting 16](#_Toc153961388)

[6. Azure Policies 16](#_Toc153961389)

[7. Configuration Templates 16](#_Toc153961390)

[Production Traffic Manager Profile 16](#_Toc153961391)

[Production Azure Public DNS Zone 17](#_Toc153961392)

[8. Acceptance 18](#_Toc153961393)

# Overview

This document covers the baseline design for the Traffic Manager 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 Traffic Manager 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 Traffic Manager.

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 Traffic Manager 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 |
| **TTL** | Time to Live |
| **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 Traffic Manager 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 was relevant. There was also guidance for operational excellence, however this overlapped with Reliability so this section has been left blank to reduce repetition.

For security there were no additional controls in the Department of Health controls, and the MSB has been referenced.

For this service there is only a single configuration template that can be used as this is a regional service that is inherently built as platinum. The details of backend configurations of the profile will depend on the applications and services that will consume it. The configuration includes setup of the Azure Public DNS zone that accompanies the Traffic Manager profile.

# Resource Cost

The pricing for Azure Traffic Manager is based on the number of DNS queries that it receives[[2]](#footnote-3). Each endpoint that is monitored also incurs a cost, and the rate varies depending on if said resource resides within Azure or externally.

|  |  |
| --- | --- |
| Pricing Item | Cost per million queries |
| First 1 billion DNS queries/month | $ 0.814 |
| Over 1 billion DNS queries/month | $0.565 |
| **Pricing Item** | **Cost per Azure endpoint/month** |
| Basic health checks | $0.543 |
| Fast interval health checks add-on | $1.506 |
| **Pricing Item** | **Cost per external endpoint/month** |
| Basic health checks | $0.814 |
| Fast interval health checks add-on | $3.012 |
| **Pricing Item** | **Cost per million data points processed** |
| Data points processed | $3.012 |

Table 2: Pricing Construct for Traffic Manager

Azure DNS also incurs a cost as follows:

|  |  |
| --- | --- |
| Pricing Item | Cost per zone per month |
| First 25 hosted DNS zones | $0.753 |
| Additional hosted DNS zones (over 25) | $0.151 |
| **Pricing Item** | **Cost per million** |
| First billion DNS queries/month | $0.603 |
| Additional DNS queries (over 1 billion)/month | $0.302 |

Table 3: Pricing Construct for Azure DNS Zone

# 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

### Traffic Manager Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | If the Time to Live (TTL) interval of the DNS record is too long, consider adjusting the health probe timing or DNS record TTL. | Yes | Yes | IaC | At deployment |
| **R2** | Implement a custom page to use as a health check for your Traffic Manager. | Yes | No | Governance and application specific designs | At deployment of application |
| **R3** | Evaluate the three different traffic routing methods. | Yes | No | Governance | At deployment |
| **R4** | Consider nested Traffic Manager profiles. | Yes | No | Application specific designs | At deployment of application |

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

### Traffic Manager Cost Optimisation Checklist

There is no WAF guidance for Cost Optimisation for Azure Traffic Manager. As such this section has been left blank.

## 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

### Traffic Manager Operational Excellence Checklist

The guidance for Operational Excellence overlaps with the guidance for reliability. As such this section has been left blank to avoid overlapping.

## 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

### Traffic Manager Performance Efficiency Checklist

There is no WAF guidance for Performance Efficiency for Azure Traffic Manager. As such this section has been left blank.

## 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 relevant Microsoft Security Controls incl

* LT-4: Enable logging for security investigation

### Traffic Manager Security Checklist

For Traffic Manager there are no Department of Health controls that provide requirements beyond the Microsoft Security Baselines. As such they will not be referenced here.

# Architecture Summary

## Resource Overview

Azure Traffic Manager is a DNS-based traffic load-balancer which can distribute the traffic of public-facing applications across regions[[7]](#footnote-8). It directs client requests to service endpoints based on the routing method configured. It will also monitor the health of endpoints. It is inherently resilient to failure as it is a global service and will remain operational even with an entire region failure.

Alongside the Traffic Manager there will be an Azure Public DNS zone that will handle the resolution of the Traffic Manager service in Azure. The following shows the flow of DNS resolutions in this process:

Figure 1: Flow of DNS resolution with Traffic Manager

## Configuring Public DNS Zones

Azure Public DNS is simple to create. Any domain can be used such as ambulance.vic.gov.au for example. Once the Public Zone is created, the name servers will be present. These will need to be registered with the DNS registrar[[8]](#footnote-9). Once registered, a CNAME can be created for Traffic Manager in this zone for the relevant application or service.

### Routing Methods Overview

There are several options for routing configurations in Traffic Manager:

* [**Priority**](https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#priority-traffic-routing-method)**:** a primary service endpoint will be chosen for all traffic. Multiple backup endpoints can be included in case the primary endpoint is unavailable.
* [**Weighted**](https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#weighted)**:** distributes traffic across a set of endpoints based on their weight. Set the weight the same to distribute evenly across all endpoints.
* [**Performance**](https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#performance)**:** to be used when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.
* [**Geographic**](https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#geographic)**:**  direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. This routing method aids in meeting data sovereignty mandates, content localization and user experience and measuring traffic from different regions.
* [**Multivalue**](https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#multivalue)**:** used for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, all healthy endpoints are returned.
* [**Subnet**](https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods#subnet)**:** this method maps a set of end-user IP address ranges to a specific endpoint.

## RBAC

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

|  |  |
| --- | --- |
| Role Name | Description |
| Traffic Manager Contributor | Lets you manage Traffic Manager profiles, but does not let you control who has access to them. |

Table 5: 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 Traffic Manager 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.

### DNS TTL

Design Reference: [Table 2](#_Traffic_Manager_Reliability) – R1

**Design Decision:** the default settings be used unless otherwise specific by an application design. If there is an existing value in the current F5 infrastructure this will be used instead of the generic values suggested by Microsoft for Traffic Manager.

**Design Justification:** The generic value for DNS TTL is 60 seconds with a 30 second probing interval. The generic tolerated failures are 3, which means that a service must be down for approximately 5 minutes before the failover kicks in. Reducing these settings may result in unnecessary failovers as some services may restore rapidly or a probe may fail unexpectedly.

Note that for a specific implementation if there is an existing value in the F5 infrastructure for DNS TTL and health checks, these should be used instead of the generic values here.

### Custom pages

**Design Reference:** [Table 2](#_Traffic_Manager_Reliability) – R2

**Design Decision:** Custom pages will be incorporated as a part of application landing zone designs that consume Traffic Manager.

**Design Justification:** Custom pages are a common practice within applications as an extra path that can be used for monitoring and performing application specific checks. It is best practice to include these.

### Routing Methods

**Design Reference:** [Table 2](#_Traffic_Manager_Reliability) – R3

**Design Decision**: Utilise the Priority method for Disaster Recovery, and Weighted if distribution across endpoints is required. Limit use of other methods as they can add complexity and administrative overhead. These should be used by exception.

**Design Justification**: The Priority method is recommended for simple failover setups and will be applicable to most Disaster Recovery scenarios for Ambulance Victoria and is the recommended option.

The Weighted method should be used for distribution across endpoints that require load balancing for DNS but are not for Disaster Recovery region failover as the Priority method is.

The Performance, Geographic, MultiValue and Subnet methods are not currently relevant to Ambulance Victoria. They may be used if required for a specific application but are not strictly necessary at this stage. It would be best to limit the routing methods to Priority and Weighted for simplicity.

### Nested Profiles

**Design Reference:** [Table 2](#_Traffic_Manager_Reliability) – R4

**Design Decision:** Nested profiles will not be accounted for as the default.

**Design Justification:** Nesting profiles increases the complexity of the Traffic Manager configuration. For simple failover scenarios this is not required. However, if there is an application specific requirement that arises which does require more complex routing systems, then this can be approved by exception for that application design.

### Diagnostics

**Design Reference:** MSB – LT-4

**Design Decision:** diagnostic logs will be enabled for Traffic Manager

**Design Justification:** logging is mandatory as per the Microsoft Security Benchmark as well as the DH Controls list.

**Design Details:** The allLogs and AllMetrics diagnostics will be enabled and sent to the central Log Analytics Workspace in Australia Southeast. Although Traffic Manager is not bound to a region, Australia Southeast is the Primary region and as such the logs will be sent there.

### Alerting

**Design Reference:**  MSB – LT-4

**Design Decision:** the Queries by endpoint returned alert will be configured if an application or service is deemed to require it. The “endpoint status by endpoint” will be configured as default for each service using the Traffic Manager instance. app

**Design Justification:** The Queries by endpoint returned metric will be captured, however an alert is not required unless by exception or a specific design requires it due to an expected high level of traffic impacting costs. The Endpoint status alert will be configured as it aids in understanding the health of backend services. This needs to be enabled for each service that uses Traffic Manager.

# Azure Policies

There are no specific Azure Policies required that relate to Azure Traffic Manager.

# Configuration Templates

There is no distinction for Traffic Manager between service tiers or even regions as this is a global service. As such there is only one template to be followed, and the details of configurations will be application or backend service specific.

### Production Traffic Manager Profile

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Subscription | AV ALZ [NAME] Subscription |
| Resource Group | rg-prd-ause-[appname]-[workload]-01 |
| Name | tm-prd-[appname]-[workload]-01 |
| URL | http://tm-prd-[appname]-[workload]-01.trafficmanager.net |
| Routing Method: | [Priority/Weighted] |
| DNS TTL: | 60 seconds |
| **Endpoint Monitoring Settings** | |
| Protocol: | <HTTP/HTTPS/TCP> |
| Port: | <port> |
| Path: | <TCP: null -or- HTTP: /> |
| **Fast Endpoint Failover Settings** | |
| Probing Interval: | 30 seconds |
| Tolerated number of Failures: | 3 |
| Probe Timeout | 10 seconds |
| **Endpoint Configuration** |  |
| Name: | tmp-<resource\_name> |
| Type: | <Azure Endpoint/External Endpoint/Nested Endpoint> |
| Target Resource Type: | <Cloud Service/App Service/App Service Slot/Public IP address> |
| Target Resource/Public IP: | <insert\_value> |
| Priority | <insert\_value> |
| Custom Header Settings: | <insert\_or\_remove> |
| Health Checks | Enabled |
| **Diagnostic Settings** |  |
| Logs to be captured | allLogs  AllMetrics |
| Log Analytics Workspace | law-prd-ause-mgmt-01 |

Table 6: Service Configuration Template

### Production Azure Public DNS Zone

|  |  |  |
| --- | --- | --- |
| Configuration Item | Configuration Details | |
| Subscription | AV ALZ Connectivity | |
| Name | e.g. ambulance.vic.gov.au | |
| Is this a child domain | No | |
| Name Servers | Available after creation | |
| Record set | Name | [Application Name] |
| Type | CNAME |
| Alias Record | No |
| Subscription | AV ALZ [NAME] Subscription |
| Alias | tmp-prd-[appname]-[workload]-01.trafficmanager.net |
| TTL | 1 |
| TTL Unit | hour |

# 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 | 2.1 |

**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/traffic-manager/ [↑](#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/traffic-manager/traffic-manager-overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/dns/dns-delegate-domain-azure-dns [↑](#footnote-ref-9)