**CORE SERVICE DESIGN:**

**Route Tables**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Route Tables Core Service Design |
| **File Name** | Ambulance Victoria – Route Tables Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 14/12/2023 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Anthony Nardone |  |  |
| **Authorised** | Daniela Nikolic |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 14/12/2023 |

Table of Contents

[1. Overview 5](#_Toc153456378)

[1.1 Purpose and Audience 5](#_Toc153456379)

[1.2 Scope and Key Deliverables 5](#_Toc153456380)

[1.3 Glossary and Definitions 6](#_Toc153456381)

[2. Executive Summary 7](#_Toc153456382)

[3. Resource Cost 7](#_Toc153456383)

[4. WAF and Security Control Alignment 8](#_Toc153456384)

[4.1 Reliability 8](#_Toc153456385)

[4.1.1 Overview 8](#_Toc153456386)

[4.1.2 Route Tables Reliability Checklist 8](#_Toc153456387)

[4.2 Cost Optimisation 9](#_Toc153456388)

[4.2.1 Overview 9](#_Toc153456389)

[4.2.2 Route Tables Cost Optimisation Checklist 9](#_Toc153456390)

[4.3 Operational Excellence 9](#_Toc153456391)

[4.3.1 Overview 9](#_Toc153456392)

[4.3.2 Route Tables Operational Excellence Checklist 9](#_Toc153456393)

[4.4 Performance Efficiency 10](#_Toc153456394)

[4.4.1 Overview 10](#_Toc153456395)

[4.4.2 Route Tables Performance Efficiency Checklist 10](#_Toc153456396)

[4.5 Security 10](#_Toc153456397)

[4.5.1 Overview 10](#_Toc153456398)

[4.5.2 Route Tables Security Checklist 10](#_Toc153456399)

[5. Architecture Summary 11](#_Toc153456400)

[5.1 Resource Overview 11](#_Toc153456401)

[5.2 Solution Diagram 12](#_Toc153456402)

[5.3 RBAC 13](#_Toc153456403)

[5.4 Design Decisions and Justifications 13](#_Toc153456404)

[5.4.1 Route Table Subnet Association 13](#_Toc153456405)

[5.4.2 Secure Network Architecture 13](#_Toc153456406)

[6. Azure Policies 13](#_Toc153456407)

[7. Configuration Templates 14](#_Toc153456408)

[7.1 Primary Region Spoke Route Table 14](#_Toc153456409)

[7.2 Secondary Region Spoke Route Table 14](#_Toc153456410)

[7.3 Hub Network Route Table Updates 15](#_Toc153456411)

[8. Acceptance 16](#_Toc153456412)

# Overview

This document covers the baseline design for the Route Tables 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 Route Table 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 Route Tables.

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 Route Tables 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 Route Tables 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. It was found that Reliability and Security pillars were applicable.

For this service the main baseline configurations include:

* Each Route Table must be applied to all Virtual Network Subnets
* Each spoke Route Table will have the following baseline routes:

(Primary Region) Australia Southeast Baseline Route Table:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address Prefix | Next hop type | Next hop IP address |
| default-to-fw | 0.0.0.0/0 | Virtual Appliance | 10.253.16.4 |
| secured-to-fw | 10.253.0.0/20 | Virtual Appliance | 10.253.16.4 |

(Secondary Region) Australia East Baseline Route Table:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address Prefix | Next hop type | Next hop IP address |
| default-to-fw | 0.0.0.0/0 | Virtual Appliance | 10.253.144.4 |
| secured-to-fw | 10.253.128.0/20 | Virtual Appliance | 10.253.144.4 |

* Propagate gateway routes must be set to **No**
* A work item to update the Connectivity hub route tables including any subnet route tables such as DMZ or Shared. This must be done for every new subnet must be done for every new network. The details of this have been captured in the Configuration Templates section.
* Any additional user-defined routes bypassing hub networks for specific traffic patterns or scenarios not covered by this document must be approved as an exception before implementing.

Note that due to the nature of this resource there is no distinction between Platinum, Gold, Silver, or Bronze tiers.

# Resource Cost

As of December 2023, there are no additional charges for creating route tables in Microsoft Azure[[2]](#footnote-3).

# 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

### Route Tables Reliability Checklist

Presented below is a reliability checklist for route tables in Azure, offering guidance to ensure correct configuration.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **R1** | Ensure the communication between Azure PaaS services that have been injected into a Virtual Network is locked down within the Virtual Network using user-defined routes (UDRs) and network security groups (NSGs). | Yes | Yes | IaC | At deployment of Virtual Network |

Table 2: 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

### Route Tables Cost Optimisation Checklist

There is no specific Cost Optimisation guidance for Route Tables as there is no cost associated with them.

## 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

### Route Tables Operational Excellence Checklist

There is no specific guidance for Operational Excellence for Route Tables.

## 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

### Route Tables Performance Efficiency Checklist

There is no specific guidance for Performance Efficiency for Route Tables.

## 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.

### Route Tables Security Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | Establish, maintain and manage a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. Ensure explicit “deny all” is used on systems to prevent unauthorised outbound connections to the internet. | Yes | Yes | IaC | At Deployment |

Table 3: Security Checklist Summary

# Architecture Summary

## Resource Overview

Route Tables, also known as User-Defined Routes, are resources that allow the user to override the default Microsoft routing[[7]](#footnote-8). This allows you greater control over virtual network traffic, and ensures that flow meets relevant security requirements, such as passing through the Firewall.

Each subnet must have an associated Route Table. The default routes for each region are listed in the [Configuration Templates](#_Configuration_Templates_1) section. Additionally, each time a new spoke network is added, the hub networks must have some of their Route Tables updated so that the new spoke networks have their routes propagated successfully throughout the network.

The Route Tables must be configured correctly both in their own spoke, as well as in the hub networks, to ensure the symmetric routing is upheld through the Azure Firewall.

In some cases, special routes will be required for Azure PaaS instances or any other non-standard routes. For Azure PaaS requirements Microsoft typically has guidance on the route required, such as for Azure Application Gateways and APIM. These routes are fine to be added so long as the design is approved and endorsed by the appropriate parties within Ambulance Victoria, and there is no other option to make the system operational.

The same is considered for special network routes such as ranges associated to an NVA or foreign networks that are not learnt as system routes. Again these will be included in the design phase for the deployment and added as approved.

## Solution Diagram



Figure 1: Generic networking diagram with Route Tables

## RBAC

For creation of Route Tables, the specific roles that can be applied are as follows:

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

Table 4: 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 Route Tables 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.

### Route Table Subnet Association

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

**Design Decision:** Every subnet will have an associated Route Table.

**Design Justification:** To ensure that routing functions properly, and that each subnet has traffic move through the Firewall when it leaves that network, it is required to have a Route Table attached with the baseline routes that have already been defined.

### Secure Network Architecture

**Design Reference:** Table 3 – [S1](#_Route_Tables_Security)

**Design Decision:** The default routes will send traffic through the Azure Firewall.

**Design Justification:** As a part of a secure network architecture, all default traffic (0.0.0.0/0) should be sent through the Firewall for inspection. Additionally, any traffic destined to leave its own network should also go through the Firewall for inspection. The Configuration Template section details the base routes that should be applied to all new networks to ensure this control is met.

# Azure Policies

There are no Azure Policies relating to Route Tables that must be applied.

# Configuration Templates

## Primary Region Spoke Route Table

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Name | rt-[env]-ause-[appname]-[workload]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia Southeast |
| Resource Group | rg-[env]-ause-[appname]-[workload]-01 |
| Virtual Network | vnet-[env]-ause-[appname]-01 |
| Associated Subnet | sn-[env]-ause-[appname]-[workload]-01 |
| **Routes** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address Prefix | Next hop type | Next hop IP address |
| default-to-fw | 0.0.0.0/0 | Virtual Appliance | 10.253.16.4 |
| secured-to-fw | 10.253.0.0/20 | Virtual Appliance | 10.253.16.4 |

## Secondary Region Spoke Route Table

|  |  |
| --- | --- |
| Configuration Item | Configuration Details |
| Name | rt-[env]-auea-[appname]-[workload]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia East |
| Resource Group | rg-[env]-auea-[appname]-[workload]-01 |
| Virtual Network | vnet-[env]-auea-[appname]-01 |
| Associated Subnet | sn-[env]-auea-[appname]-[workload]-01 |
| **Routes** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address Prefix | Next hop type | Next hop IP address |
| default-to-fw | 0.0.0.0/0 | Virtual Appliance | 10.253.144.4 |
| secured-to-fw | 10.253.128.0/20 | Virtual Appliance | 10.253.144.4 |

## Hub Network Route Table Updates

In each region there is a hub network that has several subnets. Of these the following must be updated for every new spoke network in that region:

Primary Region:

* rt-prd-ause-gateway
* rt-prd-ause-shared

Secondary Region:

* rt-prd-auea-gateway
* rt-prd-auea-shared

The format of the route updates will follow the below, with some existing examples shown:

**Primary Region**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address Prefix | Next hop type | Next hop IP address |
| [appname]-[env]-to-fw | New Vnet IP Range | Virtual Appliance | 10.253.16.4 |
| edw-prd-to-fw | 10.253.40.0/24 | Virtual Appliance | 10.253.16.4 |
| perim-npd-to-fw | 10.253.52.0/22 | Virtual Appliance | 10.253.16.4 |

**Secondary Region**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Address Prefix | Next hop type | Next hop IP address |
| [appname]-[env]-to-fw | New Vnet IP Range | Virtual Appliance | 10.253.16.4 |
| edw-prd-dr-to-fw | 10.253.168.0/24 | Virtual Appliance | 10.253.16.4 |
| perim-dr-to-fw | 10.253.52.0/22 | Virtual Appliance | 10.253.16.4 |

Note that in the above example there are multiple Disaster Recovery environments for the EDW application, so it has two environment variables in the Secondary Region Route Table.

# 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://azuremarketplace.microsoft.com/en/marketplace/apps/Microsoft.RouteTable?tab=Overview [↑](#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/virtual-network/virtual-networks-udr-overview [↑](#footnote-ref-8)