atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Dominic Panzera |
| **Email** | [Dominic.panzera@ambulance.vic.gov.au](mailto:Dominic.panzera@ambulance.vic.gov.au) |
| **Telephone** |  |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| **Title** | Ambulance Victoria – Virtual Network Core Service Design |
| **File Name** | Ambulance Victoria Virtual Network Core Service Design v2.0.docx |
| **Version** | 2.0 |
| **Status** | Updated |
| **Release Date** | 08/01/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 17/11/2023 |
| 1.1 | Minor Updates | Include RBAC, Azure Policy, Billing and Cost sections. Update WAF tables to show Enforcement Option and Applicability. | 3-4, 7-10, 13-15, 20 | 28/11/2023 |
| 1.2 | Additional Updates | CSB Controls | 13 | 29/11/2023 |
| 2.0 | Final update | Minor Changes | 9, 15, 17, 19 | 08/01/2024 |

Table of Contents

[1. Overview 5](#_Toc155611772)

[1.1 Purpose and Audience 5](#_Toc155611773)

[1.2 Scope and Key Deliverables 5](#_Toc155611774)

[1.3 Glossary and Definitions 6](#_Toc155611775)

[2. Executive Summary 7](#_Toc155611776)

[3. Resource Cost 7](#_Toc155611777)

[4. WAF and Security Control Alignment 8](#_Toc155611778)

[4.1 Reliability 8](#_Toc155611779)

[4.1.1 Overview 8](#_Toc155611780)

[4.1.2 Virtual Network Reliability Checklist 8](#_Toc155611781)

[4.2 Cost Optimisation 11](#_Toc155611782)

[4.2.1 Overview 11](#_Toc155611783)

[4.2.2 Virtual Network Cost Optimisation Checklist 11](#_Toc155611784)

[4.3 Operational Excellence 11](#_Toc155611785)

[4.3.1 Overview 11](#_Toc155611786)

[4.3.2 Virtual Network Operational Excellence Checklist 11](#_Toc155611787)

[4.4 Performance Efficiency 12](#_Toc155611788)

[4.4.1 Overview 12](#_Toc155611789)

[4.4.2 Virtual Network Performance Efficiency Checklist 12](#_Toc155611790)

[4.5 Security 13](#_Toc155611791)

[4.5.1 Overview 13](#_Toc155611792)

[4.5.2 Virtual Network Security Checklist 13](#_Toc155611793)

[5. Architecture Summary 15](#_Toc155611794)

[5.1 Resource Overview 15](#_Toc155611795)

[5.2 RBAC 15](#_Toc155611796)

[5.3 Solution Diagram 17](#_Toc155611797)

[5.4 Design Decisions and Justifications 18](#_Toc155611798)

[5.4.1 Hub and Spoke Topology 18](#_Toc155611799)

[5.4.2 Public IPs 18](#_Toc155611800)

[5.4.3 DDoS Protection 18](#_Toc155611801)

[5.4.4 Forced Tunnelling 19](#_Toc155611802)

[5.4.5 Subnet Control 19](#_Toc155611803)

[5.4.6 Private Endpoints 19](#_Toc155611804)

[5.4.7 Service Endpoints 20](#_Toc155611805)

[5.4.8 Custom DNS 20](#_Toc155611806)

[5.4.9 Monitoring and Logging 20](#_Toc155611807)

[5.4.10 Separation of Environments 21](#_Toc155611808)

[6. Azure Policies 21](#_Toc155611809)

[7. Configuration Templates 22](#_Toc155611810)

[7.1 Primary Region Virtual Network 22](#_Toc155611811)

[7.2 Secondary Region Virtual Network 24](#_Toc155611812)

[8. Acceptance 26](#_Toc155611813)

# Overview

This document covers the baseline design for the Virtual Network 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 Virtual Network 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 Virtual Network.

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 to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum 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 Virtual Network core service.

The key deliverables for this are:

* This design document to outline the service definition Level 2 baseline standards.
* Technical Configuration templates define 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 |
| **Vnet** | Virtual Network |
| **Snet** | Subnet |

Table 1: Glossary and Definitions

# Executive Summary

This design covers the baseline standards for the Virtual Network 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.

Considering the Microsoft WAF Pillars, it was found that only Reliability and Security were relevant for the virtual network service. Performance Efficiency and Operational Excellence had identical controls to Reliability and so those sections have been left blank to remove overlap. There was no guidance on cost optimisation for virtual networks.

The Virtual Networks main baseline configurations include:

* Each new spoke must be peered to the central hub for that region except for a Sandbox or environment that must remain isolated.
* An NSG and Route Table must be attached to each subnet.
* Using the standard DDoS Protection when public endpoints are in the network.
* Service Endpoints will not be enabled by default.
* Custom DNS will be defined based on the actual DNS servers.
* Azure Monitor is enabled by default and additional diagnostic logs will be forwarded to the central log analytics workspace for that region.

# Resource Cost

Virtual Networks are free of charge as an individual resource in Azure[[2]](#footnote-3). Traffic is what incurs charges, with inbound and outbound traffic being charged at both ends of network peers. The charging construct is shown below:

|  |  |
| --- | --- |
| Pricing Item | Cost per GB |
| Inbound traffic within same region | $0.016 |
| Outbound traffic within same region | $0.016 |
| Inbound traffic across regions | $0.142 |
| Outbound traffic across regions | $0.142 |

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

### Virtual Network Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **R1** | Use Azure DDoS Standard Protection Plans to protect all public endpoints hosted within customer Virtual Networks. | Yes | Yes | IaC | At deployment |
| **R2** | Enterprise customers must plan for IP addressing in Azure to ensure there's no overlapping IP address space across considered on-premises locations and Azure regions. | Yes | No | Governance | At deployment |
| **R3** | Use IP addresses from the address allocation for private internets (Request for Comment (RFC) 1918). Note that the Department of Health dictates IP address Schema so will constrain available IP ranges for allocation. | Yes | No | Governance | At deployment |
| **R4** | For environments with limited private IP addresses (RFC 1918) availability, consider using IPv6. | No | No | N/A | N/A |
| **R5** | Don't create unnecessarily large Virtual Networks (for example: /16) to ensure there's no unnecessary waste of IP address space. | Yes | No | Governance | At deployment |
| **R6** | Don't create Virtual Networks without planning the required address space in advance. | Yes | No | Governance | At deployment |
| **R7** | Don't use public IP addresses for Virtual Networks, especially if the public IP addresses don't belong to the customer. | Yes | Yes | Azure Policy | At deployment |
| **R8** | Use VNet Service Endpoints to secure access to Azure Platform as a Service (PaaS) services from within a customer VNet. | Yes | No - conflicts with R15, R16 | IaC | At deployment |
| **R9** | To address data exfiltration concerns with Service Endpoints, use Network Virtual Appliance (NVA) filtering and VNet Service Endpoint Policies for Azure Storage. | Yes | No | IaC | At deployment |
| **R10** | Don't implement forced tunnelling to enable communication from Azure-to-Azure resources. | Yes | Yes – to be handled by route table | IaC for Route Tables | At deployment of Route Table |
| **R11** | Access Azure PaaS services from on-premises through ExpressRoute Private Peering. (Read in conjunction with R12) | Yes | No – already in place and to be defined in ExpressRoute core service design | IaC for ExpressRoute | At deployment of ExpressRoute |
| **R12** | To access Azure PaaS services from on-premises networks when VNet injection or Private Link aren't available, use ExpressRoute with Microsoft Peering when there are no data exfiltration concerns. | Yes | No – already in place and to be defined in ExpressRoute core service design | IaC for ExpressRoute | At deployment of ExpressRoute |
| **R13** | Don't replicate on-premises perimeter network (also known as DMZ, demilitarized zone, and screened subnet) concepts and architectures into Azure. | Yes | No | Governance | Operational |
| **R14** | 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 |
| **R15** | Don't use VNet Service Endpoints when there are data exfiltration concerns, unless NVA filtering is used. | Yes | Yes | IaC | At deployment |
| **R16** | Don't enable VNet Service Endpoints by default on all subnets. | 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[[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

### Virtual Network Cost Optimisation Checklist

There is no specific Cost Optimisation guidance for virtual networks themselves in the context of the Well Architected Framework. Some guidance exists for other network resources such as Application Gateways, Private Endpoints, and the running cost of the services themselves, but this should be managed in their respective core service design document.

As such there is no analysis in this section for Virtual Networks.

## 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

### Virtual Network Operational Excellence Checklist

The guidance for Operational Excellence under WAF for Virtual Networks are all items identical to those covered under the Reliability section of this document, so this section will not be filled in to avoid duplication.

However, to support Operational Excellence in general there will be in the [Configuration Templates](#_Configuration_Templates) section and IaC templates to reduce human error and improve speed of deployments and repeatability when Virtual Networks are required.

## 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

### Virtual Network Performance Efficiency Checklist

There are no specific Performance Efficiency requirements in the Well Architected Framework for Virtual Networks. However, for monitoring performance of virtual networks, Azure Monitor is enabled by default for network insights. Additional diagnostic logs will also be configured and forwarded to the central log analytics workspace.

## 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

As a security baseline, Ambulance Victoria are required to meet the Microsoft Security Benchmarks at a minimum. The relevant security controls can be found in the DH MSCB Control Mapping Gap Analysis document (version 0.5 at the time of writing this document).

The relevant network security controls from CSB are:

* NS-1: Establish network segmentation boundaries
* NS-2: Secure cloud native services with network controls
* NS-5: Deploy DDOS protection
* NS-9: Connect on-premises or cloud network privately

In addition to the above 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.

### Virtual Network Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S2** | 12.3.1 | Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers. | Yes | Yes | IaC | At deployment |
| **S3** | 16.3.4 | Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate intrusion and/or compromise of data. | Yes | Yes | IaC | Operational - Daily |
| **S4** | 20.1.2 | 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 | No - to be defined in NSG Core Service Design | IaC for NSGs | At deployment |
| **S5** | 20.1.3 | Establish and maintain architecture diagram(s) and/or other network system documentation. | Yes | No | N/A | Operational – review overall architecture quarterly |
| **S6** | 21.2.1 | Perform traffic filtering between network segments, where appropriate - the sensitivity of data needs to be taken into consideration. | Yes | No - to be defined in NSG Core Service Design | IaC for NSGs | At deployment |
| **S7** | 21.2.2 | Collect network traffic flow logs and/or network traffic to review and alert upon from network devices. | Yes | No - to be defined in NSG Core Service Design | IaC for NSGs | At deployment |
| **S8** | 24.2.3 | Maintain separate environments for production and non-production systems. | Yes | Yes | IaC | At deployment |

Table 4: Security Checklist Summary

# Architecture Summary

## Resource Overview

Virtual Networks is one of the most fundamental services to Azure[[7]](#footnote-8). They are required to facilitate communication between Azure resources, the internet, and between On-Premises resources. This section references additional resources such as NSGs and Route Tables as being connected to subnets. Note that more detailed requirements for NSGs and Route Tables will be managed in their respective core services design documents.

For Ambulance Victoria specifically, to preserve symmetric routing with the Azure Firewall, the Route Tables, also known as UDRs or User Defined Routes, will need to be configured in a specific method. All traffic leaving the spoke will be routed to the Azure Firewall, which will have its own Route Table in the hub network to manage traffic flow outside of Azure and to other spokes within Azure.

## RBAC

For the Virtual Network resource, 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 5: RBAC roles relevant for this core service

These are the least privileged roles required for access to only manage Virtual Networks in Azure. For Ambulance Victoria, there are no classic networks in use, as such only Network Contributor is relevant.

## Solution Diagram



Figure 1: Generalised Virtual Network diagram

The example above shows a generic virtual network in a spoke subscription with a disaster recovery spoke in a separate resource group under the same subscription. The virtual networks are peered to their respective hubs with a NSG and Route Table attached to each subnet. Azure Monitor, custom DNS and diagnostic settings are enabled.

## 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 Virtual Network 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.

### Hub and Spoke Topology

**Document Reference:** Table 2 - [S4, S8](#_Virtual_Network_Security)

**Design Decision:** all additional spoke virtual networks should be peered to the respective hub for that region (except for anything that is required to be isolated such as a Sandbox).

**Design Justification:** Note that technically this architecture is already in place and previously approved for the CAF build of the Enterprise Landing Zone. The Hub-and-Spoke topology supports segregation of applications and systems, as well as separation of environments. This also allows RBAC to be managed more effectively by splitting the spokes of each application and environment out. The only exception is for Sandboxes or isolated environments that will not be peered to the hub.

**Design** **Details:** Every new spoke must be peered to the hub network for its respective region (Australia Southeast as Primary, and Australia East as Secondary/Disaster Recovery). The parameters and baseline values for virtual networks will be defined in the accompanying Configuration Template document.

### Public IPs

**Document Reference:** Table 1-[R7](#_Virtual_Network_Reliability)

**Design Decision**: Public IPs will not be deployed within a virtual network by default

**Design Justification:** To minimize the attack surface public IPs will not be deployed with the virtual network module and will not be designed as a standard module. Any application designs requiring direct internet connectivity will require exemptions and security assessment. The creation of Public IP resources is also currently blocked by Azure Policy, so any attempts to deploy one without an exemption will be denied.

### DDoS Protection

**Document references:**

Table 1-[R1](#_Virtual_Network_Reliability)

CSB Control NS-5

**Design Decision**: Use the existing DDoS Network Protection plan (ddos-prd-hub-01) under the AZ 3 Tenant which should be used across multiple subscriptions and virtual networks.

Use DDoS Protection on any networks that do require public interfaces.

**Design Justification**: DDoS Network Protection Standard is required for additional protection for the virtual networks and public internet facing resources.

**Design Details:** A central DDoS Protection plan (Standard tier) will be applied to all networks and services that have a public IP or public interface. There is already a centralised DDoS Protection plan in the AV ALZ Connectivity subscription, and this will be applied to any virtual networks in future that require a public resource.

### Forced Tunnelling

**Document Reference:** Table 1-[R10](#_Virtual_Network_Reliability)

**Design Decision:** forced tunnelling will not be used for Azure-to-Azure resource communication. In other words there will be no forced tunnelling for intra-vnet traffic.

**Design Justification:** using forced tunnelling for resources on the same network, or even across networks within Azure, is extremely inefficient and cost intensive. It will also result in unnecessary latency, and any security concerns will be addressed with NSGs and Route Tables. As such there is no reason to use forced tunnelling for resources within Azure trying to reach each other.

### Subnet Control

**Document Reference:** Table 1-[R14](#_Virtual_Network_Reliability)

**Design Decision:** Assign an NSG and a Route Table to each subnet

**Design Justification:** For security and the control of traffic flow it is necessary to have an NSG and a Route Table attached to each subnet. The IaC template will include references for NSGs and Route Tables for each subnet, and Azure Policy will audit for any subnets that do not have an NSG attached that should be reviewed periodically as a part of regular governance process. The detailed configuration requirements of NSGs and Route Tables will be defined in their respective core services design documents.

### Private Endpoints

**Document Reference:** CSB Control NS-2

**Design Decision:** Use Private Endpoints where available.

**Design Justification:** The most secure method of accessing Azure resources is via Private Endpoint or Private Link functionality. Details of how Private Endpoints should be configured will be further defined in the Private Endpoint core service design document.

### Service Endpoints

**Document Reference:** Table 1–[R15, R16](#_Virtual_Network_Reliability)

**Design Decision**: Service Endpoints will not be enabled by default.

**Design Justification**: As per WAF guidance, service endpoints will not be enabled by default, and will only be added in as required by a specific application architecture. This will be a part of the Application Landing Zone design and can be added to the base Virtual Network IaC module for that specific deployment as long as the design is approved in the appropriate forums.

### Custom DNS

**Document Reference:** Table 2 - [S2](#_Virtual_Network_Security)

**Design Decision:** Ambulance Victoria will use custom DNS servers on virtual networks.

**Design Justification:** To meet security requirements this control requires the use of enterprise controlled or trusted DNS servers to be used. As such, the Domain Controllers in Azure will be used as DNS servers to manage name resolution across Azure resources. These will be defined in the [Configuration Template](#_Configuration_Templates) section of this document.

### Monitoring and Logging

**Document Reference:** Table 2 - [S3](#_Virtual_Network_Security)

**Design Decision:** Azure Monitor by default will monitor network resources. An additional diagnostic setting will be configured.

**Design Details:** Azure Monitor already provides network insights without specific configuration required[[8]](#footnote-9). Additionally, a diagnostic setting will be created to send logs to the central log analytics workspace for that region.

**Design Details:** a diagnostic setting for the available settings of allLogs and allMetrics will be selected and forwarded to the log analytics workspace designated for that region which are situated in the AV ALZ Management subscription.

### Separation of Environments

**Document Reference:** Table 2 - [S8](#_Virtual_Network_Security)

**Design Decision:** each environment for an application or service will have its own spoke. Production and Non-Production spokes will be kept separate, and communication between them will only be allowed by exception and will pass through the Azure Firewall via the Hub peering.

**Design Justification:** segregation of environments is critical as conflicts inevitably arise when production and non-production are in the same place. They have completely different purposes and will therefore require different restrictions. As such it is best practice to segregate environments.

**Design Details:** The structure of the IaC will only allow for one environment to be deployed at a time. The parameters file will dictate which environment is being deployed, and there will be one parameters file for each environment.

# Azure Policies

The only Azure Policy required is already in place to deny the creation of public IPs.

|  |  |
| --- | --- |
| Policy Name | Scope |
| Deny the creation of public IP | av management group (under Root) |

Table 6: Azure Policies

# Configuration Templates

In Azure, Virtual Networks are the primary building block for private IaaS resources as well as PaaS resources.

The address space conforms to the agreed upon network address schema as defined by Ambulance Victoria.

Diagnostic logging is enabled for all available categories and sent to Log Analytics workspace.

Note that for virtual networks there is no distinction between Service Catalog tiers as there are no specific configurations that can be applied to make the virtual networks operate meet these specific requirements.

## Primary Region Virtual Network

The configuration below is for any virtual network being deployed in the Australia Southeast (Primary) region. As a part of the current architectural standard this can be used for Production or Non-Production (Development, Testing, UAT etc.) resources. If these resources are required to be deployed into the Secondary region an exemption must be provided, and the template for Secondary Region virtual networks may be used.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Configuration Item | Configuration Details | | | |
| **Name** | vnet-[env]-ause-[appname]-01 | | | |
| **Resource Group** | rg-[env]-ause-[appname]-[workload]-01 | | | |
| **Subscription** | AV ALZ [Subscription Name] | | | |
| **Address Space** | <Allocated CIDR> | | | |
| **DDoS Protection** | Disabled | | | |
| **Firewall** | Disabled | | | |
| **DNS Servers (ordered)** | AZ2 (currently configured):  172.24.242.4  172.24.226.4  AZ3 (To be configured as the target state):  10.253.24.5  10.253.152.5 | | | |
| **Subnets** |  | | | |
|  | **Subnet Name** | | **Address Range** | |
| snet-[env]-ause-[appname]-[workload]-01 | | <CIDR> | |
| snet-[env]-ause-[appname]-[workload]-0x | | <CIDR> | |
| snet-[env]-ause-[appname]-[workload]-0x | | <CIDR> | |
| **Peering** |  | | | |
|  | **Local Peering Name**  [vnet-[env]-ause-[appname]-01](https://portal.azure.com/)-to-vnet-prd-ause-hub-01 | | | |
| **Local VNET** | **Configuration** | | **Status** |
| vnet-[env]-ause-[appname]-01 | Allow access to remote virtual network | | Enabled |
| Allow traffic forwarded from remote network | | Enabled |
| Allow local gateway to forward traffic to hub | | Disabled |
| Allow use of remote gateway | | Enabled |
| **Remote Peering Name**  vnet-prd-ause-hub-01-to-[vnet-[env]-ause-[appname]-01](https://portal.azure.com/) | | | |
| **Remote VNET** | **Configuration** | | **Status** |
| vnet-prd-ause-hub-01 | Allow access to remote virtual network | | Enabled |
| Allow traffic forwarded from remote network | | Enabled |
| Allow local gateway to forward traffic to hub | | Enabled |
| Allow use of remote gateway | | Disabled |
| **Service Endpoints** |  | | | |
|  | **Service** | | None enabled by default | |
| **Subnets** | | N/A | |
| **Private Endpoints** |  | |  | |
|  | **Service** | | Configured per service requirement | |
|  | **Subnets** | | N/A | |
| **Diagnostics** |  | |  | |
|  | **Log Analytics Workspace** | | law-prd-ause-mgmt-01 | |
|  | **Settings** | |  | |
|  | allLogs  allMetrics | | Enabled  Enabled | |

Table 7: Baseline settings for primary region

## Secondary Region Virtual Network

Network boundary to segregate the Disaster Recovery environment resources in the Secondary region.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Configuration Item | Configuration Details | | | |
| **Name** | vnet-[env]-auea-[appname]-01 | | | |
| **Resource Group** | rg-[env]-auea-[appname]-[workload]-01 | | | |
| **Subscription** | AV ALZ [Subscription Name] | | | |
| **Address Space** | <Allocated CIDR> | | | |
| **DDoS Protection** | Disabled | | | |
| **Firewall** | Disabled | | | |
| **DNS Servers (ordered)** | AZ2 (currently configured):  172.24.226.4  172.24.242.4  AZ3 (To be configured as the target state):  10.253.152.5  10.253.24.5 | | | |
| **Subnets** |  | | | |
|  | **Subnet Name** | | **Address Range** | |
| snet-[env]-auea-[appname]-[workload]-01 | | <CIDR> | |
| snet-[env]-auea-[appname]-[workload]-0x | | <CIDR> | |
| sn-[env]-auea-[appname]-[workload]-0x | | <CIDR> | |
| **Peering** |  | | | |
|  | **Local Peering Name**  [vnet-[env]-auea-[appname]-01](https://portal.azure.com/)-to-vnet-prd-auea-hub-01 | | | |
| **Local VNET** | **Configuration** | | **Status** |
| vnet-[env]-auea-[appname]-01 | Allow access to remote virtual network | | Enabled |
| Allow traffic forwarded from remote network | | Enabled |
| Allow local gateway to forward traffic to hub | | Disabled |
| Allow use of remote gateway | | Enabled |
| **Remote Peering Name**  vnet-prd-auea-hub-01-to-[vnet-[env]-auea-[appname]-01](https://portal.azure.com/) | | | |
| **Remote VNET** | **Configuration** | | **Status** |
| vnet-prd-auea-hub-01 | Allow access to remote virtual network | | Enabled |
| Allow traffic forwarded from remote network | | Enabled |
| Allow local gateway to forward traffic to hub | | Enabled |
| Allow use of remote gateway | | Disabled |
| **Service Endpoints** |  | | | |
|  | **Service** | | None enabled by default | |
| **Subnets** | | N/A | |
| **Private Endpoints** |  | |  | |
|  | **Service** | | Configured per service requirement | |
|  | **Subnets** | | N/A | |
| **Diagnostics** |  | |  | |
|  | **Log Analytics Workspace** | | law-prd-auea-mgmt-01 | |
|  | **Settings** | |  | |
|  | allLogs  allMetrics | | Enabled  Enabled | |

Table 8: Baseline settings for secondary region

# 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.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 2.0 |

**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/virtual-network/ [↑](#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-overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/network-watcher/network-insights-overview [↑](#footnote-ref-9)