**CORE SERVICE DESIGN:**

**Virtual Machine and Managed Disks**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Virtual Machine and Managed Disks Core Service Design |
| **File Name** | Ambulance Victoria – Virtual Machine and Managed Disks Core Service Design v2.1.docx |
| **Version** | 2.1 |
| **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 | 8/12/2023 |
| 2.0 | Minor Updates | Include more size information | 25, 29, 30-41 | 14/12/2023 |
| 2.1 | Minor Updates | Naming and configuration template updates | 31-38 | 08/01/2024 |

Table of Contents

[1. Overview 6](#_Toc153458031)

[1.1 Purpose and Audience 6](#_Toc153458032)

[1.2 Scope and Key Deliverables 6](#_Toc153458033)

[1.3 Glossary and Definitions 7](#_Toc153458034)

[2. Executive Summary 8](#_Toc153458035)

[3. Resource Cost 9](#_Toc153458036)

[4. WAF and Security Control Alignment 9](#_Toc153458037)

[4.1 Reliability 10](#_Toc153458038)

[4.1.1 Overview 10](#_Toc153458039)

[4.1.2 Virtual Machine and Managed Disks Reliability Checklist 10](#_Toc153458040)

[4.2 Cost Optimisation 11](#_Toc153458041)

[4.2.1 Overview 11](#_Toc153458042)

[4.2.2 Virtual Machine and Managed Disks Cost Optimisation Checklist 11](#_Toc153458043)

[4.3 Operational Excellence 12](#_Toc153458044)

[4.3.1 Overview 12](#_Toc153458045)

[4.3.2 Virtual Machine and Managed Disks Operational Excellence Checklist 12](#_Toc153458046)

[4.4 Performance Efficiency 13](#_Toc153458047)

[4.4.1 Overview 13](#_Toc153458048)

[4.4.2 Virtual Machine and Managed Disks Performance Efficiency Checklist 13](#_Toc153458049)

[4.5 Security 14](#_Toc153458050)

[4.5.1 Overview 14](#_Toc153458051)

[4.5.2 Virtual Machine and Managed Disks Security Checklist 14](#_Toc153458052)

[5. Architecture Summary 18](#_Toc153458053)

[5.1 Resource Overview 18](#_Toc153458054)

[5.1.1 Managed Disks Overview 18](#_Toc153458055)

[5.1.2 Virtual Machine Monitoring Overview 18](#_Toc153458056)

[5.2 RBAC 19](#_Toc153458057)

[5.3 Design Decisions and Justifications 20](#_Toc153458058)

[5.3.1 Flexible Scale Sets and Autoscaling 20](#_Toc153458059)

[5.3.2 Availability Zones 21](#_Toc153458060)

[5.3.3 Ephemeral Disks 21](#_Toc153458061)

[5.3.4 Maintenance Configurations 22](#_Toc153458062)

[5.3.5 Alerting 22](#_Toc153458063)

[5.3.6 Automate Power Schedules 23](#_Toc153458064)

[5.3.7 Spot VMs 23](#_Toc153458065)

[5.3.8 Virtual Machine Sizing 24](#_Toc153458066)

[5.3.9 Bastion for Remote Access 25](#_Toc153458067)

[5.3.10 Hybrid Benefits 25](#_Toc153458068)

[5.3.11 Azure Monitoring Agent 25](#_Toc153458069)

[5.3.12 VM Insights and Diagnostics 25](#_Toc153458070)

[5.3.13 Latency Reduction (Proximity Placement Groups) 26](#_Toc153458071)

[5.3.14 Virtual Machine Disk Tiers 26](#_Toc153458072)

[5.3.15 NVMe 26](#_Toc153458073)

[5.3.16 Accelerated Networking 27](#_Toc153458074)

[5.3.17 Just In Time Access 27](#_Toc153458075)

[5.3.18 Update Management 27](#_Toc153458076)

[5.3.19 Operating Systems 27](#_Toc153458077)

[5.3.20 Disk Encryption 28](#_Toc153458078)

[5.3.21 Backups 28](#_Toc153458079)

[6. Azure Policy 29](#_Toc153458080)

[7. Configuration Templates 30](#_Toc153458081)

[7.1 Available Sizes 30](#_Toc153458082)

[7.2 Platinum Production Primary Region 31](#_Toc153458083)

[7.2.1 Platinum Primary Windows VM 31](#_Toc153458084)

[7.2.2 Platinum Primary Windows VM Scale Set 31](#_Toc153458085)

[7.2.3 Platinum Primary Linux VM 32](#_Toc153458086)

[7.2.4 Platinum Primary Linux VM Scale Set 32](#_Toc153458087)

[7.3 Platinum or DR Secondary Region 33](#_Toc153458088)

[7.3.1 DR Windows VM 33](#_Toc153458089)

[7.3.2 DR Windows VM Scale Set 33](#_Toc153458090)

[7.3.3 DR Linux VM 34](#_Toc153458091)

[7.3.4 DR Linux VM Scale Set 34](#_Toc153458092)

[7.4 Gold or Silver Primary Region 35](#_Toc153458093)

[7.4.1 Gold or Silver Primary Windows VM 35](#_Toc153458094)

[7.4.2 Gold or Silver Primary Windows VM Scale Set 36](#_Toc153458095)

[7.4.3 Gold or Silver Primary Linux VM 36](#_Toc153458096)

[7.4.4 Gold or Silver Primary Linux VM Scale Set 37](#_Toc153458097)

[7.5 Bronze or Non-Production Primary Region 37](#_Toc153458098)

[7.5.1 Bronze or Non-Production Windows VM 37](#_Toc153458099)

[7.5.2 Bronze or Non-Production Linux VM 38](#_Toc153458100)

[8. Appendix – Allowed Sizes 39](#_Toc153458101)

[9. Acceptance 42](#_Toc153458102)

# Overview

This document covers the baseline design for the Virtual Machine and Managed Disks core service. The intention of this document is to define the overall resource design in isolation from a specific application. It will highlight the general process and requirements for building a Virtual Machine and Managed Disks 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 Machine and Managed Disks.

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 Virtual Machine and Managed Disks core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration template 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. |
| **IaaS** | Infrastructure as a Service |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **VM** | Virtual Machine |
| **VMSS** | Virtual Machine Scale Sets |
| **AMA** | Azure Monitoring Agent |
| **NIC** | Network Interface Card |
| **NSG** | Network Security Groups |

Table 1: Glossary and Definitions

# Executive Summary

This design covers the baseline standards for the Virtual Machine and Managed Disks 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 all pillars were relevant and had specific guidance for Virtual Machines.

For this service the main baseline configurations include:

* The (Azure Monitor Agent) will be deployed to all machines.
* VM Insights and diagnostics will be enabled by default on all machines.
* The base set of alerts will be configured on all machines.
* Azure Bastion will be used for administrative management of all machines.
* JIT functionality will be enabled for all machines.
* Disk encryption will be enabled for all machines.
* Update Manager will be used for all machines (unless an alternative strategy is required) using Maintenance Configurations for scheduling.
* Azure Backup will be enabled on all machines (until an alternative solution is implemented).
* Hybrid Benefits will be enabled where applicable on all machines.
* Accelerated networking will be enabled where applicable on all machines.

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

* The Platinum or Production (including Gold and Silver tiers) deployments will be deployed in VMSS with a minimum of 1 extra scale unit (2 in total, and more as the design requires). They will be design in Flexible Orchestration mode. Bronze or Non-Production servers can be deployed as single instances.
* The Platinum or Production (including Gold or Silver tiers) deployments will use Premium SSD disks for OS and Data Disks. Non-Production or Bronze applications can use Standard SSD.
* The patching and backup requirements will also differ, but these details will be outlined in the Backup and Update Management Core Services designs.

# Resource Cost

Costs for Virtual Machines vary based on VM Family and size, as well as the actual Windows or Linux OS licensing. The full list of prices can be found [here.](https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/)

# 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[[2]](#footnote-3). 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 Machine and Managed Disks Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **R1** | Review SLAs for virtual machines | Yes | No | Governance | At deployment |
| **R2** | Deploy using Flexible scale sets | Yes | Yes | IaC | At deployment |
| **R3** | Deploy across availability zones | Partial – if using Australia East | Yes | IaC | At deployment |
| **R4** | Install applications on Ephemeral OS disks | Yes | Yes | IaC | At deployment |
| **R5** | Use Maintenance Configuration | Yes | Partial – details covered in Update Management core service design | IaC – defined in Azure Update module | At deployment |
| **R6** | Create availability alert rules for Azure VMs. | Yes | Yes | IaC | At deployment |
| **R7** | Create agent heartbeat alert rule to verify agent health. | Yes | Yes | IaC | At deployment |
| **R8** | Configure data collection and alerting for monitoring reliability of client workflows. | Yes | Yes | IaC | At deployment |

Table 2: WAF Reliability Checklist Summar

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[3]](#footnote-4). 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 Machine and Managed Disks Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Stop VMs during off-hours | Yes | No | Governance – manual task | At deployment |
| **CO2** | Use Spot VMs when appropriate | No | No | N/A | N/A |
| **CO3** | Right-size your VMs | Yes | No | Governance | Operational – to be reviewed and remediated monthly |
| **CO4** | Configure Azure Bastion for operational access | Yes | Yes | IaC – already deployed | At deployment |
| **CO5** | Utilize Premium SSD v2 effectively | Yes | Yes | IaC | At deployment |
| **CO6** | Optimize with managed disks | Yes | Yes | IaC | At deployment |
| **CO7** | Prepay for added cost savings | Yes | No | Governance | Operational – to be reviewed annually |
| **CO8** | Use existing licensing through the hybrid benefit licensing program | Yes | Yes | IaC, Governance | At deployment |
| **CO9** | Deploy AMA | Yes | Yes | IaC | At deployment |

Table 3: WAF Cost Optimisation Checklist Summary

## 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 Machine and Managed Disks Operational Excellence Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **OE1** | Monitor and measure health | Yes | Yes | IaC | Operational – daily |
| **OE2** | Setup Azure Monitor alert rules | Yes | Yes | IaC | At deployment |
| **OE3** | Automate tasks | Yes | Yes | IaC | At deployment |
| **OE4** | Build a robust testing environment | Yes | No | Governance | Operational |
| **OE5** | Manage your quota | Yes | No | Governance | At deployment, and review overall quota quarterly |

Table 4: WAF Operational Excellence Checklist Summary

## 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[[4]](#footnote-5). This covers capacity and scalability:

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

### Virtual Machine and Managed Disks Performance Efficiency Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **PE1** | Reduce latency | Yes | Yes | IaC | At deployment |
| **PE2** | Convert disks from standard HDD to premium SSD | Yes | Yes | IaC | At deployment |
| **PE3** | Use locally attached NVMe devices | Yes | No | IaC | At deployment |
| **PE4** | Consider accelerated networking | Yes | Yes | IaC | At deployment |
| **PE5** | Use autoscaling | Yes | Yes | IaC | At deployment |

Table 5: WAF Performance Efficiency Checklist Summary

## 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[[5]](#footnote-6):

* 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.

### Virtual Machine and Managed Disks Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 2.1.1 | The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S2** | 2.1.2 | Application control is implemented on workstations and internet-facing servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S3** | 2.1.3 | Allowed and blocked executions on workstations and internet-facing servers are logged. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S4** | 2.2.1 | Application control is implemented on workstations and servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set. | Yes | No | Cylance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S5** | 2.2.2 | Microsoft’s ‘recommended block rules’ are implemented. | Yes | No | Cylance | N/A to Azure for Endpoint Management  At deployment |
| **S6** | 2.2.3 | Microsoft’s ‘recommended driver block rules’ are implemented. | Yes | No | Cylance | N/A to Azure for Endpoint Management  At deployment |
| **S7** | 2.2.4 | Application control rulesets are validated on an annual or more frequent basis. | Yes | No | Governance | N/A to Azure for Endpoint Management  Operational – to be reviewed quarterly |
| **S8** | 2.2.5 | Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected. | Yes | No | Sentinel | N/A to Azure for Endpoint Management  Operational - daily |
| **S9** | 3.2.4 | Administrative activities are conducted through jump servers. | Yes | Yes | Already deployed - Bastion | Operational |
| **S10** | 3.3.3 | Just-in-time administration is used for administering systems and applications. | Yes | Yes | IaC | At deployment |
| **S11** | 3.2.5 | Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed. | Yes | No | Governance, GPO | N/A to Azure for Endpoint Management  Operational - quarterly |
| **S12** | 3.3.4 | Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled. | Yes | No | GPO | N/A to Azure for Endpoint Management |
| **S13** | 4.1.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. | Yes | Yes | IaC – Update Manager  Governance | At deployment  Operational for Zero Day exploits |
| **S14** | 4.1.2 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. | Yes | Yes | IaC – Update Manager  Governance | At deployment |
| **S15** | 4.1.3 | A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. | Yes | Yes | Tenable | N/A to Azure for Endpoint Management  Operational |
| **S16** | 4.1.4 | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. | Yes | Yes | Tenable | N/A to Azure for Endpoint Management  Operational |
| **S17** | 4.1.5 | Operating systems that are no longer supported by vendors are replaced. | Yes | No | Governance | Operational – review quarterly |
| **S18** | 4.2.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release. | Yes | No | Governance | At deployment |
| **S19** | 4.2.2 | A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices. | Yes | No | Tenable | Operational - weekly |
| **S20** | 4.3.1 | Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within 48 hours if an exploit exists. | Yes | No | Governance | Operational for Zero Day exploits |
| **S21** | 4.3.2 | The latest release, or the previous release, of operating systems are used. | Yes | No | Governance | At deployment and operational |
| **S22** | 5.1.1 | Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. | Yes | Yes | IaC | At deployment |
| **S23** | 5.1.2 | Restoration of important data, software and configuration settings from backups to a common point of time is tested as part of disaster recovery exercises. | Yes | Yes | Governance | Operational – test quarterly |
| **S24** | 11.2.3 | Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. | Yes | Yes | IaC | At deployment |

Table 6: Security checklist summary

# Architecture Summary

## Resource Overview

Azure Virtual Machines are an on-demand compute resource that allows you the flexibility of compute power without the requirement to buy physical hardware[[6]](#footnote-7). The high-level design considerations for Virtual Machines include:

* Size and pricing
* Deployment location
* Operating System requirements
* Security and operational configurations
* Backup and recovery options

### Managed Disks Overview

Azure Managed Disks are block-level storage volumes that are consumed with Azure Virtual Machines[[7]](#footnote-8). They are inherently highly available and are supported by Azure Backup. RBAC can also be applied to individual disks.

Unmanaged disks will be deprecated by 2025 so only Managed Disks will be considered for Virtual Machines.

### Virtual Machine Monitoring Overview

Virtual Machine monitoring in Azure can be quite convoluted as there are several layers at which logs can be collected, and therefore can lead to issues such as log duplication. The four layers that monitoring and telemetry can be applied to are:

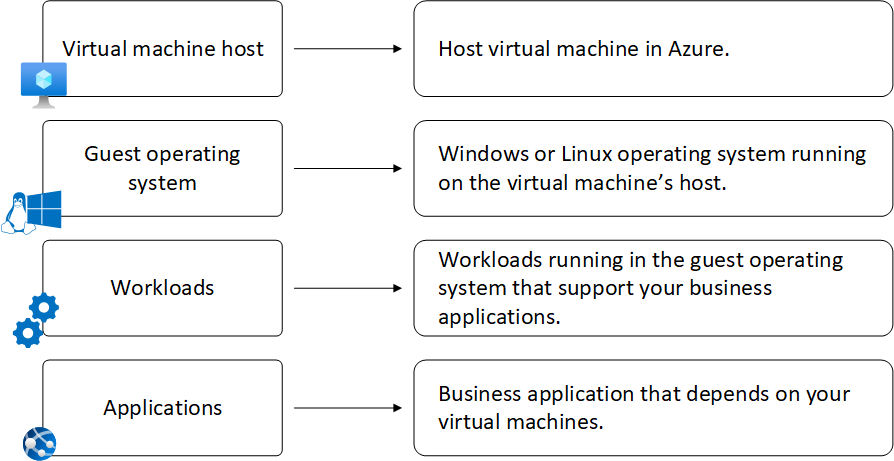


Figure 1: Monitoring and telemetry layers applicable to Virtual Machines[[8]](#footnote-9)

These layers are monitored in different ways, and for the purposes of this design the relevant layers are the Virtual Machine host and the Guest OS layer. The simplest way to configure data collection for these layers is to enable VM Insights (which requires the AMA).

## RBAC

For Virtual Machines and Managed Disks the following RBAC is applicable:

|  |  |
| --- | --- |
| **Role Name** | **Description** |
| Classic Virtual Machine Contributor | Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to. |
| Data Operator for Managed Disks | Provides permissions to upload data to empty managed disks, read, or export data of managed disks (not attached to running VMs) and snapshots using SAS URIs and Azure AD authentication. |
| Disk Backup Reader | Provides permission to backup vault to perform disk backup. |
| Disk Pool Operator | Provide permission to StoragePool Resource Provider to manage disks added to a disk pool. |
| Disk Restore Operator | Provides permission to backup vault to perform disk restore. |
| Disk Snapshot Contributor | Provides permission to backup vault to manage disk snapshots. |
| Virtual Machine Administrator Login | View Virtual Machines in the portal and login as administrator |
| Virtual Machine Contributor | Create and manage virtual machines, manage disks, install and run software, reset password of the root user of the virtual machine using VM extensions, and manage local user accounts using VM extensions. This role does not grant you management access to the virtual network or storage account the virtual machines are connected to. This role does not allow you to assign roles in Azure RBAC. |
| Virtual Machine Data Access Administrator (preview) | Manage access to Virtual Machines by adding or removing role assignments for the Virtual Machine Administrator Login and Virtual Machine User Login roles. Includes an ABAC condition to constrain role assignments. |
| Virtual Machine User Login | View Virtual Machines in the portal and login as a regular user. |
| Windows Admin Center Administrator Login | Let's you manage the OS of your resource via Windows Admin Center as an administrator. |

Table 7: 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 Virtual Machine and Managed Disks 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.

### Flexible Scale Sets and Autoscaling

**Overview**

Scale sets allow you to automatically create and manage groups of VMs that are load balanced by default[[9]](#footnote-10). The virtual machines can be spread across Availability Zones or fault domains which guarantees application resiliency. The scaling can be done in response to demand or a pre-defined schedule.

The orchestration models available are Flexible or Uniform Orchestration[[10]](#footnote-11). Microsoft recommends using the Flexible method under WAF to future proof applications for availability and scalability.

**Design Reference:** [Table 1](#_Virtual_Machine_and) – R2, [Table 4](#_Virtual_Machine_and_1), PE5

**Design Decision**: Deploy using virtual machine scale sets with flexible orchestration.

**Design Justification**:According to the Well Architected Framework even single instance Virtual Machines should be deployed in VMSS to protect applications from facing availability issues or any scaling concerns. It may not always be necessary to deploy VMs within a VMSS, such as for Non-Production or availability insensitive workloads, but is recommended for Silver, Gold and Platinum applications.

Flexible orchestration will be used instead of the Uniform Orchestration method as the Flexible mode is easier to manage, and improves upon some of the limitations of the more traditional Uniform Orchestration mode. These limitations included:

* VMSS API was different to individual VM APIs increasing deployment and operational overheads
* Lack of granular RBAC permissions at the individual VM level
* Lack of ASR and Azure Backup support

Flexible Orchestration addresses all the above concerns, increasing the security posture of the solution whilst maintaining the benefits.

### Availability Zones

**Design Reference:** [Table 1](#_Virtual_Machine_Reliability) – [R3](#_Virtual_Machine_Reliability)

**Design Decision:** Availability Zones cannot currently be used. When they are available in the Primary Region, all deployments should use Availability Zones where possible.

**Design Justification**:As Ambulance Victoria’s primary region is Australia Southeast, it is not possible to leverage Availability Zones as they are not supported by Azure in this region. When Availability Zones become available in Australia Southeast, they should be used for all deployments. The Availability Zones in Australia East will generally not be required as this region is to be used for Disaster Recovery purposes, so high availability within that region is not required. When available AZs will be leveraged for VMSS deployments.

### Ephemeral Disks

**Design Reference:** [Table 1](#_Virtual_Machine_Reliability) – R4

**Design Decision:** Ephemeral Disks will not be used.

**Design Justification:** Ephemeral disks are not generally supported for most VM sizes and are operationally more difficult to manage than the standard managed disks[[11]](#footnote-12). Data on the OS disk will be deleted if the machine requires resizing or re-redeploying. Additionally stop/start of the VM is not supported which conflicts with another WAF recommendation.

Ephemeral disks are best for stateless applications and do have decreased latency and can fast reset or reimage VMs. However, as these are not typical deployment scenarios for Ambulance Victoria they will not be used as they will only add unnecessary complexity.

### Maintenance Configurations

**Design Reference:** [Table 1](#_Virtual_Machine_Reliability) – R5

**Design Decision:** Maintenance configurations will be used for Update Management of Linux and Windows machines.

**Design Justification**:Maintenance configurations will be used for Virtual Machines (both Linux and Windows) as this is the simplest, and most automated, way to manage updates. In some cases, machines may require manual patching due to application requirements. These will be managed by the Patching team lead. Any machines that can be automatically updated will be added to their relevant Maintenance Configuration. Details of these configurations will be outlined in the Azure Update core service design.

As general guidance, Non-Production or non-critical machines will be patched close to the release date of the patch, so that any issues caused by patching will be identified prior to the patch being released to critical and Production workloads which would typically happen a week later.

### Alerting

**Design Reference:** [Table 1](#_Virtual_Machine_Reliability) – R6, R7, R8, [Table 3](#_Virtual_Machine_and_3) – OE2

**Design Decision:** Best practice Microsoft recommended alerts will be applied for each VM or VMSS. This can be done at the Subscription level for each new subscription out of Azure Monitor so that any new VM or VMSS immediately inherits the pre-defined alerts.

**Design Justification:** The below alerts will be configured for every new subscription via Azure Monitor. In this way you only need to create a handful of rules that will be applied to all Virtual Machines under that scope. Managing rules for each individual machine will add unnecessary administrative overhead.

**Design Details:** The following recommended alert rules will be applied to Virtual Machines and alerts will be distributed to the nominated e-mail address from Ambulance Victoria[[12]](#footnote-13):

* % CPU greater than 80%
* Available memory in bytes less than 1 GB
* Data Disk IOPS Consumed % greater than 95%
* OS Disk IOPS Consumed % greater than 95%
* Network in total is greater than 500GB
* Network out total is greater than 200GB
* VMAvailabilityMetric is less than 1

Additionally, the following Activity Log alert rules will be created:

* VM Stop
* VM Start
* VM Restart

### Automate Power Schedules

**Design Reference:** [Table 2](#_Virtual_Machine_and_2) – CO1

**Design Decision:** Stop VMs that do not require 24x7 operations (typically Bronze service tier).

**Design Justification**:Machines are priced on a size and usage basis. Reducing the number of hours that the machines are operational will reduce spend. This is recommended for Non-Production VMs that do not need to operate 24x7 and do not have an Ambulance Victoria Service Catalog requirement to be available constantly. This would be applicable to Bronze tiered machines.

**Design Details:** Start/Stop of Virtual Machines will be configured in the Azure Portal. The scheduling may vary per VM, but suggested the suggested schedules are:

* Stop VM after office hours (9am -5pm Monday to Friday) and on weekends.
* Stop VM on weekends only.

### Spot VMs

**Design Reference:** [Table 2](#_Virtual_Machine_and_2) – CO2

**Design Decision:** Spot VMs will not be used.

**Design Justification:** Due to the nature of spot VMs they are inherently unreliable and can be stopped and deallocated at any time. Even for Non-Production workloads this can be frustrating and concerning particularly if Non-Production is required to mimic the Production environment. There are also extremely limited sizes that are available for this scheme.

### Virtual Machine Sizing

**Design Reference:** Table 2 – CO3

**Design Decision**: Limit the families that can be deployed and review machine sizing quarterly.

**Design Justification**: Limiting the families that can be used helps operational efficiency and reduces the risk that users will deploy machines that are unnecessarily powerful for general workloads. The selected families are generally suitable for most workloads, and if an exception is required it can be requested. Choosing machines in the same family also allows for Reserved Instances to be allocated across workloads, creating efficiencies in cost savings.

Additionally, the requirement to review and remediate sizing monthly will assist in managing cost and performance as machines will be appropriately sized. Azure Advisor will recommend appropriate sizes based on performance metrics.

**Design Details**: The following is a summary of the Azure VM sizing’s and what they are applicable for typically in Azure[[13]](#footnote-14) [[14]](#footnote-15) [[15]](#footnote-16):

|  |  |  |
| --- | --- | --- |
| Family | Application | AV Use |
| A Series | Entry Level Workloads | Not recommended as Series is retiring and does not have Reserved Instances options available. |
| Bs Series | Economical burstable compute | Dev and Testing workloads only Azure Policy to restrict for Production |
| D Series | General purpose compute | Suitable for general application workloads |
| E Series | Memory optimised | Suitable for memory intensive workloads such as SAP/HANA, SQL and other relational databases |
| F Series | Compute optimised | Suitable for applications that need high CPU without requirements for high memory such as batch processing and web servers. |
| L Series | Storage optimised | Suitable for workloads that have extreme throughput requirements. To be restricted across platform. |

Table 8: Summary of Azure VM Sizes and Applicability

The most applicable to Ambulance Victoria will be the D Series machines which are suitable for most applications and workloads. Specifically, new machines will be assumed to be the Size D2s\_v3 (2vCPU and 8GB Memory) unless otherwise required by the application design.

### Bastion for Remote Access

**Design Reference:** [Table 2](#_Virtual_Machine_and_2) – CO4

**Design Decision:** Bastion will be used for management of Azure VMs, unless there is a specific functionality that cannot be met by Azure Bastion. In these cases the existing Jumphosts will be used.

**Design Justification:** Bastion is already in place under the original CAF landing zone implementation, and this will continue to be used as the native and secure solution for remote management of IaaS Virtual Machines in Azure. The network that the VM is deployed into must be peered to the hub for Bastion access to function as it has been centralised. There are some services that Azure Bastion does not have and existing Jumphosts have additional applications. Bastion will be used primarily for administration, unless there is a specific requirement to use a Jumphost.

### Hybrid Benefits

**Design Reference:** [Table 2](#_Virtual_Machine_and_2) – CO8

**Design Decision:** Hybrid Benefits will be enabled if Ambulance Victoria confirm eligibility to the scheme based on existing On-Premise licenses.

**Design Justification:** Hybrid benefits can be enabled at the creation of the Virtual Machine which means the cost of the VM is only for the compute and not the license of the OS running over it. A minimum of 8-core is required per VM. The savings can be up to 49% which makes the scheme worthwhile particularly when moving VMs from On-Premise into Azure as the licensing will be retained.

### Azure Monitoring Agent

**Design Reference:** [Table 2](#_Virtual_Machine_and_2) – CO9

**Design Decision:** Azure Monitoring Agent will be deployed to all Virtual Machines.

**Design Justification:** A pre-requisite to being able to fully monitor and collect logs on Azure Virtual Machines is to have the Azure Monitoring Agent installed. Given these are security mandates, and the previous Azure Log Analytics Agent is becoming redundant, the AMA must be used.

### VM Insights and Diagnostics

**Design Reference:** [Table 3](#_Virtual_Machine_and_3) –OE1

**Design Decision**: VM Insights will be enabled by default for all machines and diagnostics will be enabled.

**Design Justification**: It is a requirement to monitor health and performance of resources in Azure, particularly Virtual Machines which are running business critical workloads. VM Insights will be enabled as it onboards the VM to Azure Monitor rapidly and will install the AMA which is required for other log collections.

VM Insights does not capture and forward all logs such as guest logs. To do this the diagnostics extension will also be enabled and data sent to a diagnostic storage account resource within the same subscription.

Change tracking and Inventory will also be enabled which also use the AMA. Logs will all be forwarded to the Log Analytics Workspace within the same region that the VM has been deployed into.

### Latency Reduction (Proximity Placement Groups)

**Design Reference:** [Table 4](#_Virtual_Machine_and_1) – PE1

**Design Decision:** use proximity placement groups if applications are extremely latency sensitive.

**Design Justification:** Proximity placement groups are not generally required as the latency between Azure machines is not generally an issue for most applications. However, if reduced latency is required, VMs associated with a specific application or service can be placed into the same proximity placement group.

### Virtual Machine Disk Tiers

**Design Reference: Table 3 – D4**

**Design Decision:** Use Standard SSD for Non-Production and Premium SSD for Production workloads.

**Design Justification:** Non-production workloads do not require Premium disks for operation as they do not have the same low latency, always-on and throughput requirements. Premium SSD and Premium SSD v2 can both be used, though v2 is more costly and caters for applications that have high IOPS and low latency requirements. Premium SSD will be assumed as the default for Production.

### NVMe

Design Reference: [Table 4](#_Virtual_Machine_and_1) – PE3

**Design Decision:** NVMe will not be enabled as standard.

**Design Justification:** NVMe refers to Non-volatile memory express, which is a protocol that enables fast data transfer between servers and storage systems[[16]](#footnote-17). It is only available for few, memory-optimised SKUs that are not generally used at Ambulance Victoria, and only applicable to Linux systems. If it is required for an application an exemption to standard architecture should be raised and approved.

### Accelerated Networking

**Design Reference:** [Table 4](#_Virtual_Machine_and_1) – PE4

**Design Decision:** Accelerated Networking will be enabled by default if available for the VM size and supported OS versions.

**Design Justification:** Accelerated Networking enhances the throughput of an application at no extra cost. It is not available in all sizes and not available for legacy OS versions. As such it will be enabled whenever possible as the default option.

### Just In Time Access

**Design Reference:** [Table 5](#_Virtual_Machine_and_4) – S10

**Design Decision:** JIT will be enabled on all Virtual Machines.

**Design Justification:** it is a security mandate that data just-in-time access is enabled for machines.

### Update Management

**Design Reference:** [Table 5](#_Virtual_Machine_and_4) – S13, S14, S18

**Design Decision:** Azure Update Management will be used as the cloud-native solution for updates management.

**Design Justification:** Updates must be installed to maintain security posture for all Virtual Machines.

**Design Details:** the specific details of the update settings for each machine will be defined in the Azure Update Management core service design document.

### Operating Systems

**Design Reference:** [Table 5](#_Virtual_Machine_and_4) – S21

**Design Decision:** the latest available Operating System will be used, unless application specific requirements require an earlier version.

**Design Justification: it is a security requirement to use the most up-to-date version of Operating Systems as they are inherently more secure.**

**Design Details:** at the time of writing, the latest OS version for Windows is 2022 Data Centre for servers. For Linux the latest release of each variant will be used such as RHEL 8.

### Disk Encryption

**Design Reference:** [Table 5](#_Virtual_Machine_and_4) – S24

**Design Decision:** Azure Disk Encryption will be enabled on all disks.

**Design Justification:** it is a security mandate that data is encrypted at rest so ADE will be enforced on all disks (both OS and Data Disks).

### Backups

**Design Reference:** [Table 5](#_Virtual_Machine_and_4) – S22

**Design Decision:** Azure Backup will be used to backup Virtual Machines, or any other solution that may be used (e.g. Commvault).

**Design Details:** The specific backup policies will be defined in the Recovery Services Vault Core Service Design. Generally, there will be a policy for Non-Production and a policy for Production servers that is more frequent and stringent.A retention period of 7 years is assumed to be the standard unless otherwise defined by Ambulance Victoria.

# Azure Policy

The following built-in policy will be leveraged with the following restrictions applied:

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy Name** | **Scope** | **Restricted Families** | **Allowed Families** |
| Allowed Virtual Machine SKUs | Av Prod | A Series  B Series  B Series v2  F Series v2  D Series v2  F Series  L Series  M Series | D-Series v5  D-Series v4  D-Series v3  E Series v4  E Series v5 |
| Allowed Virtual Machine SKUs | Av Non-Prod | As above but excluding B-Series as these are suitable for Non-Production. | B-Series  B-Series v2  D-Series v3  D-Series v4  D-Series v5  E Series v4  E Series v5 |

**Table 6: Azure Policies**

The above machines have been restricted based on previous recommendations and quote limitations. They are non-standard sizes or perform functions that can be achieved with other families.

# Configuration Templates

The following section details the configuration details for each major deployment requirement that Ambulance Victoria will have for Azure IaaS Virtual Machines.

## Available Sizes

The following sizes and families will be available to use. The base recommendation is to use D2s\_v3 and use larger sizes as required.

* D-Series v3
* D-Series v4
* D-Series v5
* E Series v4
* E Series v5
* B Series (Non-Production)
* B Series v2 (Non-Production)

E Series are recommended where the application requires memory intensive workloads. Otherwise D-Series is generally applicable. The differences in version are in the underlying hardware, with v5 currently the latest. The following is proposed for configurations:

* Platinum tier – use v5 series where available
* Gold or Silver tier – use v4 series where available
* Bronze – use v3 series or lower where available

Full details of available sizes can be found in the Appendix.

## Platinum Production Primary Region

### Platinum Primary Windows VM

The following shows the base configuration details for a Windows Virtual Machine. Additional information about the VMSS is in the next table.

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PWV-AZM-[APPCODE]01 |
| **Resource Group** | rg-prd-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Scale Set** | pwvmss-AZM-[APPCODE]01 |
| **Operating System** | 2022-datacenter-azure-edition-smalldisk |
| **VM Size** | Small: Standard\_D2s\_v5 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v5 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v5 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-prd-ause-[appname]-[workload]-01 |
| **Subnet** | sn-prd-ause-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Premium SSD) |
| **Data Disk(s)** | PWV-AZM-[APPCODE]01\_DataDisk (Premium SSD)  64GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-prd-ause-[appname]-mgmt -01 |
| **Azure Backup Policy** | Production Platinum Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

### Platinum Primary Windows VM Scale Set

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | pwvmss-AZM-[APPCODE]01 |
| **Resource Group** | rg-prd-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Orchestration** | Flexible |
| **Security Type** | Standard |
| **Virtual Network** | vnet-prd-ause-[appname]-[workload]-01 |
| **Subnet** | sn-prd-ause-[appname]-[workload]-0# |
| **Initial Instance Count** | 2 |
| **Scaling Policy** | Manual |
| **Scale-In Policy** | Default – balance across availability zones and fault domains |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **Health** | Enable application health monitoring |

### Platinum Primary Linux VM

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PLV-AZM-[APPCODE]01 |
| **Resource Group** | rg-prd-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Scale Set** | plvmss-AZM-[APPCODE]01 |
| **Operating System** | RHEL 8.0/Ubuntu 22.04/Debian 12/Oracle Linux 9 |
| **VM Size** | Small: Standard\_D2s\_v5 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v5 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v5 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-prd-ause-[appname]-[workload]-01 |
| **Subnet** | sn-prd-ause-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Premium SSD) |
| **Data Disk(s)** | PLV-AZM-[APPCODE]01\_DataDisk (Premium SSD)  64GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-prd-ause-[appname]-mgmt -01 |
| **Azure Backup Policy** | Production Platinum Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

### Platinum Primary Linux VM Scale Set

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | plvmss-AZM-[APPCODE]01 |
| **Resource Group** | rg-prd-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Orchestration** | Flexible |
| **Security Type** | Standard |
| **Virtual Network** | vnet-prd-ause-[appname]-[workload]-01 |
| **Subnet** | sn-prd-ause-[appname]-[workload]-0# |
| **Initial Instance Count** | 2 |
| **Scaling Policy** | Manual |
| **Scale-In Policy** | Default – balance across availability zones and fault domains |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **Health** | Enable application health monitoring |

## Platinum or DR Secondary Region

### DR Windows VM

The following shows the base configuration details for a Windows Virtual Machine. Additional information about the VMSS is in the next table.

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PWV-AZS-[APPCODE]01 |
| **Resource Group** | rg-dr-auea-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Scale Set** | pwvmss-AZS-[APPCODE]01 |
| **Operating System** | 2022-datacenter-azure-edition-smalldisk |
| **VM Size** | Small: Standard\_D2s\_v5 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v5 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v5 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-dr-auea-[appname]-[workload]-01 |
| **Subnet** | sn-dr-auea-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Premium SSD) |
| **Data Disk(s)** | PWV-AZM-[APPCODE]01\_DataDisk (Premium SSD)  64GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-prd-auea-[appname]-mgmt -01 |
| **Azure Backup Policy** | Production Platinum Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

### DR Windows VM Scale Set

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | pwvmss-AZS-[APPCODE]01 |
| **Resource Group** | rg-dr-auea-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia East |
| **Orchestration** | Flexible |
| **Security Type** | Standard |
| **Virtual Network** | vnet-dr-auea-[appname]-[workload]-01 |
| **Subnet** | sn-dr-auea-[appname]-[workload]-0# |
| **Initial Instance Count** | 2 |
| **Scaling Policy** | Manual |
| **Scale-In Policy** | Default – balance across availability zones and fault domains |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **Health** | Enable application health monitoring |

### DR Linux VM

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PLV-AZS-[APPCODE]01 |
| **Resource Group** | rg-dr-auea-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Scale Set** | plvmss-AZS-[APPCODE]01 |
| **Operating System** | RHEL 8.0/Ubuntu 22.04/Debian 12/Oracle Linux 9 |
| **VM Size** | Small: Standard\_D2s\_v5 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v5 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v5 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-dr-auea-[appname]-[workload]-01 |
| **Subnet** | sn-dr-auea-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Premium SSD) |
| **Data Disk(s)** | PLV-AZM-DataDisk-[APPCODE]-01 (Premium SSD)  128GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-dr-auea-[appname]-mgmt -01 |
| **Azure Backup Policy** | Production Platinum Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

### DR Linux VM Scale Set

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | plvmss-AZM-[APPCODE]01 |
| **Resource Group** | rg-dr-auea-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia East |
| **Orchestration** | Flexible |
| **Security Type** | Standard |
| **Virtual Network** | vnet-dr-auea-[appname]-[workload]-01 |
| **Subnet** | sn-dr-auea-[appname]-[workload]-0# |
| **Initial Instance Count** | 2 |
| **Scaling Policy** | Manual |
| **Scale-In Policy** | Default – balance across availability zones and fault domains |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **Health** | Enable application health monitoring |

## Gold or Silver Primary Region

### Gold or Silver Primary Windows VM

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PWV-AZM-[APPCODE]01 |
| **Resource Group** | rg-[env]-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Scale Set** | pwvmss-AZM-[APPCODE]01 |
| **Operating System** | 2022-datacenter-azure-edition-smalldisk |
| **VM Size** | Small: Standard\_D2s\_v4 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v4 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v4 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-[env]-ause-[appname]-[workload]-01 |
| **Subnet** | sn-[env]-ause-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Premium SSD) |
| **Data Disk(s)** | PWV-AZM-[APPCODE]01\_DataDisk (Premium SSD)  64GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-prd-ause-[appname]-mgmt -01 |
| **Azure Backup Policy** | Silver/Gold Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

### Gold or Silver Primary Windows VM Scale Set

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | pwvmss-AZM-[APPCODE]01 |
| **Resource Group** | rg-[env]-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Orchestration** | Flexible |
| **Security Type** | Standard |
| **Virtual Network** | vnet-[env]-ause-[appname]-[workload]-01 |
| **Subnet** | sn-[env]-ause-[appname]-[workload]-0# |
| **Initial Instance Count** | 2 |
| **Scaling Policy** | Manual |
| **Scale-In Policy** | Default – balance across availability zones and fault domains |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **Health** | Enable application health monitoring |

### Gold or Silver Primary Linux VM

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PLV-AZM-[APPCODE]01 |
| **Resource Group** | rg-[env]-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Scale Set** | plvmss-AZM-[APPCODE]01 |
| **Operating System** | RHEL 8.0/Ubuntu 22.04/Debian 12/Oracle Linux 9 |
| **VM Size** | Small: Standard\_D2s\_v4 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v4 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v4 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-[env]-ause-[appname]-[workload]-01 |
| **Subnet** | sn-[env]-ause-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Premium SSD) |
| **Data Disk(s)** | PLV-AZM-[APPCODE]01\_DataDisk (Premium SSD)  64GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-prd-ause-[appname]-mgmt -01 |
| **Azure Backup Policy** | Gold/Silver Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

### Gold or Silver Primary Linux VM Scale Set

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | plvmss-AZM-[APPCODE]01 |
| **Resource Group** | rg-[env]-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Region** | Australia Southeast |
| **Orchestration** | Flexible |
| **Security Type** | Standard |
| **Virtual Network** | vnet-[env]-ause-[appname]-[workload]-01 |
| **Subnet** | sn-[env]-ause-[appname]-[workload]-0# |
| **Initial Instance Count** | 2 |
| **Scaling Policy** | Manual |
| **Scale-In Policy** | Default – balance across availability zones and fault domains |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **Health** | Enable application health monitoring |

## Bronze or Non-Production Primary Region

### Bronze or Non-Production Windows VM

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PWV-AZM-[APPCODE]01 |
| **Resource Group** | rg-[env]-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Operating System** | 2022-datacenter-azure-edition-smalldisk |
| **VM Size** | Small: Standard\_D2s\_v3 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v3 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v3 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-[env]-ause-[appname]-[workload]-01 |
| **Subnet** | sn-[env]-ause-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Standard SSD) |
| **Data Disk(s)** | PWV-AZM-[APPCODE]01\_DataDisk (Standard SSD)  64GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-[env]-ause-[appname]-mgmt -01 |
| **Azure Backup Policy** | Non-Production Bronze Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

### Bronze or Non-Production Linux VM

|  |  |
| --- | --- |
| **Configuration Item** | **Configuration Details** |
| **Name** | PLV-AZM-[APPCODE]01 |
| **Resource Group** | rg-[env]-ause-[appname]-[workload]-01 |
| **Subscription** | AV ALZ [Subscription Name] |
| **Operating System** | RHEL 8.0/Ubuntu 22.04/Debian 12/Oracle Linux 9 |
| **VM Size** | Small: Standard\_D2s\_v3 (2vCPU and 8GB Memory)  Medium: Standard\_D16s\_v3 (16vCPU and 64GB Memory)  Large: Standard\_D48s\_v3 (48vCPU and 192 GB Memory) |
| **IP Addresses** | [Assigned at creation] |
| **Virtual Network** | vnet-[env]-ause-[appname]-[workload]-01 |
| **Subnet** | sn-[env]-ause-[appname]-[workload]-0# |
| **OS Disk** | 127 GiB (Standard SSD) |
| **Data Disk(s)** | PLV-AZM-[APPCODE]01\_DataDisk (Standard SSD)  64GB |
| **Agents Installed** | Tenable  AMA |
| **VM Insights** | Enabled |
| **Monitoring** | Boot diagnostics enabled with managed storage account |
| **JIT** | Enabled |
| **Update Management Maintenance Configuration** | mc-[env]-ause-[appname]-mgmt -01 |
| **Azure Backup Policy** | Non-Production Bronze Policy |
| **Disk Encryption** | ADE on all Disks |
| **Bastion Access** | Enabled |
| **Hybrid Benefits** | Enabled/Disabled |

# Appendix – Allowed Sizes

D-Series v3[[17]](#footnote-18)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Size | vCPU | Memory: GiB | Temp storage (SSD) GiB | Max data disks | Max NICs/ Expected network bandwidth (Mbps) |
| Standard\_D2s\_v3 | 2 | 8 | 16 | 4 | 2/1000 |
| Standard\_D4s\_v3 | 4 | 16 | 32 | 8 | 2/2000 |
| Standard\_D8s\_v3 | 8 | 32 | 64 | 16 | 4/4000 |
| Standard\_D16s\_v3 | 16 | 64 | 128 | 32 | 8/8000 |
| Standard\_D32s\_v3 | 32 | 128 | 256 | 32 | 8/16000 |
| Standard\_D48s\_v3 | 48 | 192 | 384 | 32 | 8/24000 |
| Standard\_D64s\_v3 | 64 | 256 | 512 | 32 | 8/30000 |

D-Series v4[[18]](#footnote-19)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Size | vCPU | Memory: GiB | Temp storage (SSD) GiB | Max data disks | Max NICs/ Expected network bandwidth (Mbps) |
| Standard\_D2s\_v4 | 2 | 8 | Remote Storage Only | 4 | 2/5000 |
| Standard\_D4s\_v4 | 4 | 16 | Remote Storage Only | 8 | 2/10000 |
| Standard\_D8s\_v4 | 8 | 32 | Remote Storage Only | 16 | 4/12500 |
| Standard\_D16s\_v4 | 16 | 64 | Remote Storage Only | 32 | 8/12500 |
| Standard\_D32s\_v4 | 32 | 128 | Remote Storage Only | 32 | 8/16000 |
| Standard\_D48s\_v4 | 48 | 192 | Remote Storage Only | 32 | 8/24000 |
| Standard\_D64s\_v4 | 64 | 256 | Remote Storage Only | 32 | 8/30000 |

D-Series v5[[19]](#footnote-20)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Size | vCPU | Memory: GiB | Temp storage (SSD) GiB | Max data disks | Max NICs/ Expected network bandwidth (Mbps) |
| Standard\_D2s\_v5 | 2 | 8 | Remote Storage Only | 4 | 2/12500 |
| Standard\_D4s\_v5 | 4 | 16 | Remote Storage Only | 8 | 2/12500 |
| Standard\_D8s\_v5 | 8 | 32 | Remote Storage Only | 16 | 4/12500 |
| Standard\_D16s\_v5 | 16 | 64 | Remote Storage Only | 32 | 8/12500 |
| Standard\_D32s\_v5 | 32 | 128 | Remote Storage Only | 32 | 8/16000 |
| Standard\_D48s\_v5 | 48 | 192 | Remote Storage Only | 32 | 8/24000 |
| Standard\_D64s\_v5 | 64 | 256 | Remote Storage Only | 32 | 8/30000 |
| Standard\_D96s\_v5 | 96 | 384 | Remote Storage Only | 32 | 8/35000 |

E Series v4[[20]](#footnote-21)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Size | vCPU | Memory: GiB | Temp storage (SSD) GiB | Max data disks | Max NICs/ Expected network bandwidth (Mbps) |
| Standard\_E2s\_v4 | 2 | 8 | Remote Storage Only | 4 | 2/12500 |
| Standard\_E4s\_v4 | 4 | 16 | Remote Storage Only | 8 | 2/12500 |
| Standard\_E8s\_v4 | 8 | 32 | Remote Storage Only | 16 | 4/12500 |
| Standard\_E16s\_v4 | 16 | 64 | Remote Storage Only | 32 | 8/12500 |
| Standard\_E20s\_v4 | 20 | 160 | Remote Storage Only | 32 | 8/12500 |
| Standard\_E32s\_v4 | 32 | 128 | Remote Storage Only | 32 | 8/16000 |
| Standard\_D48s\_v4 | 48 | 192 | Remote Storage Only | 32 | 8/24000 |
| Standard\_D64s\_v4 | 64 | 256 | Remote Storage Only | 32 | 8/30000 |
| Standard\_D96s\_v4 | 96 | 384 | Remote Storage Only | 32 | 8/35000 |

E Series v5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Size | vCPU | Memory: GiB | Temp storage (SSD) GiB | Max data disks | Max NICs/ Expected network bandwidth (Mbps) |
| Standard\_E2s\_v5 | 2 | 8 | Remote Storage Only | 4 | 2/12500 |
| Standard\_E4s\_v5 | 4 | 16 | Remote Storage Only | 8 | 2/12500 |
| Standard\_E8s\_v5 | 8 | 32 | Remote Storage Only | 16 | 4/12500 |
| Standard\_E16s\_v5 | 16 | 64 | Remote Storage Only | 32 | 8/12500 |
| Standard\_E20s\_v5 | 20 | 160 | Remote Storage Only | 32 | 8/12500 |
| Standard\_E32s\_v5 | 32 | 128 | Remote Storage Only | 32 | 8/16000 |
| Standard\_D48s\_v5 | 48 | 192 | Remote Storage Only | 32 | 8/24000 |
| Standard\_D64s\_v5 | 64 | 256 | Remote Storage Only | 32 | 8/30000 |
| Standard\_D96s\_v5 | 96 | 384 | Remote Storage Only | 32 | 8/35000 |
| Standard\_E104is\_v5 | 104 | 672 | Remote Storage Only | 64 | 8/100000 |

# 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 | 2.1 |

**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://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/virtual-machines/overview [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/virtual-machines/managed-disks-overview [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/overview [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-orchestration-modes [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/azure/virtual-machines/ephemeral-os-disks [↑](#footnote-ref-12)
12. https://learn.microsoft.com/en-us/azure/azure-monitor/vm/tutorial-monitor-vm-alert-recommended [↑](#footnote-ref-13)
13. https://learn.microsoft.com/en-us/azure/virtual-machines/sizes [↑](#footnote-ref-14)
14. https://orangematter.solarwinds.com/2023/01/31/azure-virtual-machine-types/ [↑](#footnote-ref-15)
15. https://www.smikar.com/azure-vms-sizes/ [↑](#footnote-ref-16)
16. https://learn.microsoft.com/en-us/azure/virtual-machines/enable-nvme-interface [↑](#footnote-ref-17)
17. https://learn.microsoft.com/en-us/azure/virtual-machines/dv3-dsv3-series [↑](#footnote-ref-18)
18. https://learn.microsoft.com/en-us/azure/virtual-machines/dv4-dsv4-series [↑](#footnote-ref-19)
19. https://learn.microsoft.com/en-us/azure/virtual-machines/dv5-dsv5-series [↑](#footnote-ref-20)
20. https://learn.microsoft.com/en-us/azure/virtual-machines/ev4-esv4-series [↑](#footnote-ref-21)