**CORE SERVICE DESIGN:**

**Azure Monitor and Insights**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Azure Monitor and Insights Core Service Design |
| **File Name** | Ambulance Victoria – Azure Monitor and Insights Core Service Design v2.0.docx |
| **Version** | 2.0 |
| **Status** | Updated |
| **Release Date** | 14/02/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 8/02/2024 |
| 2.0 | Minor Updates | Naming  convention | 18 | 14/02/2024 |

Table of Contents

[1. Overview 5](#_Toc158801735)

[1.1 Purpose and Audience 5](#_Toc158801736)

[1.2 Scope and Key Deliverables 5](#_Toc158801737)

[1.3 Glossary and Definitions 6](#_Toc158801738)

[2. Executive Summary 7](#_Toc158801739)

[3. Resource Cost 8](#_Toc158801740)

[4. WAF and Security Control Alignment 8](#_Toc158801741)

[4.1 Reliability 9](#_Toc158801742)

[4.1.1 Overview 9](#_Toc158801743)

[4.1.2 Azure Monitor and Insights Reliability Checklist 9](#_Toc158801744)

[4.2 Cost Optimisation 9](#_Toc158801745)

[4.2.1 Overview 9](#_Toc158801746)

[4.2.2 Azure Monitor and Insights Cost Optimisation Checklist 9](#_Toc158801747)

[4.3 Operational Excellence 10](#_Toc158801748)

[4.3.1 Overview 10](#_Toc158801749)

[4.3.2 Azure Monitor and Insights Operational Excellence Checklist 10](#_Toc158801750)

[4.4 Performance Efficiency 11](#_Toc158801751)

[4.4.1 Overview 11](#_Toc158801752)

[4.4.2 Azure Monitor and Insights Performance Efficiency Checklist 11](#_Toc158801753)

[4.5 Security 12](#_Toc158801754)

[4.5.1 Overview 12](#_Toc158801755)

[5. Architecture Summary 13](#_Toc158801756)

[5.1 Resource Overview 13](#_Toc158801757)

[5.1.1 Azure Monitor Insights 14](#_Toc158801758)

[5.2 RBAC 15](#_Toc158801759)

[5.3 Design Decisions and Justifications 16](#_Toc158801760)

[5.3.1 Configuring General Logging and Metrics 16](#_Toc158801761)

[5.3.2 Configuring VM Insights 16](#_Toc158801762)

[5.3.3 Configuring Container Insights 16](#_Toc158801763)

[5.3.4 Application Insights 17](#_Toc158801764)

[5.3.5 Configuring Network Insights 17](#_Toc158801765)

[6. Azure Policies 18](#_Toc158801766)

[7. Configuration Templates 18](#_Toc158801767)

[7.1 Primary Region Azure Application Insights (Platinum, Gold, Silver) 18](#_Toc158801768)

[7.2 Secondary Region Azure Application Insights (Platinum, Gold, Silver) 18](#_Toc158801769)

[8. Acceptance 19](#_Toc158801770)

# Overview

This document covers the baseline design for the Azure Monitor and Insights 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 Azure Monitor and Insights 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 Azure Monitor and Insights.

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 Azure Monitor and Insights core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |

Table 1: Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Azure Monitor and Insights 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 Security and Operational Excellence were relevant.

Note that this design covers Azure Monitor as well as the Insights features for these specific services:

* Application Insights
* Container Insights
* VM Insights
* Network Insights

For this service the main baseline configurations include:

* Azure Monitor as a service is enabled on the platform by default.
* The specialised Insights will be enabled for each relevant service.
* Any “Insights” service enabled will send logs to the central Log Analytics Workspace within that region.

There is no difference in configuration of Azure Monitor or Insights across service tiers as they are just collection and analysis agents. The only note to make is that they can be considered optional for Bronze services if this data is not required for collection and analysis.

Note that Alerting is not covered in detail in this design, and will be treated separately in its own design document.

# Resource Cost

The collection of standard metrics and activity logs are provided at no cost. Log costs are associated with the Log Analytics Workspace that is being used, and these costs are covered in the Log Analytics Core Service design.

Metric costs are shown below:

|  |  |  |
| --- | --- | --- |
| Feature | Free units included | Price |
| Platform Metrics Ingestion8 | Unlimited | Free |
| Custom metrics ingestion (preview)8 | None | **$0.243** / 10 million samples ingested |
| Platform and custom metric queries (preview) | First 1,000,000 API calls per month | **$0.015169** / 1,000 API calls |

Table 2: Pricing construct for metrics

# 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

### Azure Monitor and Insights Reliability Checklist

There is no guidance for Azure Monitor or Insights under the Reliability pillar.

## 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

### Azure Monitor and Insights Cost Optimisation Checklist

There is no guidance for Azure Monitor under the Cost Optimisation pillar of the Microsoft Well-Architected Framework. The only Cost Optimisation guidance provided relates to the underlying Log Analytics Workspaces that collects the data, and this has already been covered in the Log Analytics Workspace design document.

## 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

### Azure Monitor and Insights Operational Excellence Checklist

There is no guidance for Azure Monitor under the Operational Excellence pillar of the Microsoft Well Architected Framework.

There is guidance for Application Insights[[4]](#footnote-5):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Design | Enforcement Option | Applicability |
| **OE1** | Configure Application Insights to monitor the availability and responsiveness of your web application. | Yes | No | Governance | Operational – during application deployment |
| **OE2** | Evaluate Java codeless application monitoring for your Java-based application development stack. | Yes | No | Governance | Operational – during application deployment |
| **OE3** | Configure sampling in Application Insights. | Yes | No | Governance | Operational – during application deployment |
| **OE4** | Record custom events and metrics from sites and services in Application Insights. | Yes | No | Governance | Operational – during application deployment |
| **OE5** | Use Application Insights to ingest existing log traces from common libraries, such as ILogger, Nlog, and log4Net. | Yes | No | Governance | Operational – during application deployment |
| **OE6** | Become familiar with the Application Insights quotas and limits. | Yes | No | Governance | Operational – at deployment |
| **OE7** | Review the need for custom analysis. Use Application Insights data with tools such as Azure Dashboards or Power BI. | Yes | No | Governance | Operational – review additional toolsets required |
| **OE8** | Separate data across Application Insights resources. | Yes | No | Governance | Operational – during application landing zone design |

Table 4: Application Insights 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[[5]](#footnote-6). This covers capacity and scalability:

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

### Azure Monitor and Insights Performance Efficiency Checklist

There is no guidance for Azure Monitor or Insights under the Performance Efficiency pillar of the Microsoft Well-Architected Framework.

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[6]](#footnote-7):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

The following Microsoft Security Benchmark controls are applicable to Azure Monitor[[7]](#footnote-8):

* IM-1: Use centralized identity and authentication system.
* IM-3: Manage application identities securely and automatically.
* DP-3: Encrypt sensitive data in transit.
* DP-4: Enable data at rest encryption by default.
* LT-4: Enable logging for security investigation.

# Architecture Summary

## Resource Overview

Azure Monitor is a native monitoring service that provides collection, analysis, and alerting features for services that leverage the capability[[8]](#footnote-9). It has the ability to monitor the following source types:

* Applications
* Virtual machines
* Guest operating systems
* Containers including Prometheus metrics
* Databases
* Security events in combination with Azure Sentinel
* Networking events and health in combination with Network Watcher
* Custom sources that use the APIs to get data into Azure Monitor

The Data Stores vary depending on the type of data collected6:

|  |  |
| --- | --- |
| Data Store | Description |
| Azure Monitor Metrics | Metrics are numerical values that describe an aspect of a system at a particular point in time. Azure Monitor Metrics is a time-series database, optimized for analyzing time-stamped data. Azure Monitor collects metrics at regular intervals. Metrics are identified with a timestamp, a name, a value, and one or more defining labels. |
| Azure Monitor Logs | Logs are recorded system events. Logs can contain different types of data, be structured or free-form text, and they contain a timestamp. Azure Monitor stores structured and unstructured log data of all types in Azure Monitor Logs. |
| Traces | Distributed tracing allows you to see the path of a request as it travels through different services and components. Azure Monitor gets distributed trace data from instrumented applications. The trace data is stored in a separate workspace in Azure Monitor Logs. |
| Changes | Changes are a series of events in your application and resources. They're tracked and stored when you use the Change Analysis service, which uses Azure Resource Graph as its store. Change Analysis helps you understand which changes, such as deploying updated code, may have caused issues in your systems. |

Table 6: Summary of Data Stores for Azure Monitor

The following shows the destinations of various data that can be collected via Azure Monitor[[9]](#footnote-10):

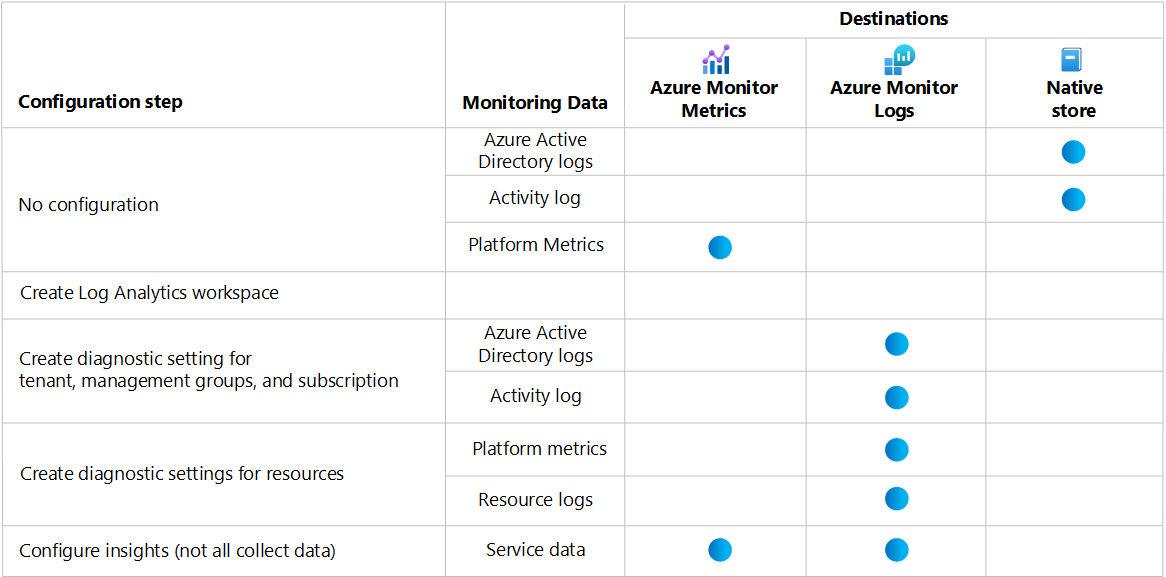


Figure 1: Summary of Azure Monitor sources and destinations

### Azure Monitor Insights

Some services in Azure have a more detailed and curated monitoring experience available that can be configured[[10]](#footnote-11):

|  |  |
| --- | --- |
| Insight | Description |
| Application Insights | Application Insights monitors the availability, performance, and usage of your web applications. |
| Container Insights | Container Insights gives you performance visibility into container workloads that are deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service. Container Insights collects container logs and metrics from controllers, nodes, and containers that are available in Kubernetes through the Metrics API. After you enable monitoring from Kubernetes clusters, these metrics and logs are automatically collected for you through a containerized version of the Log Analytics agent for Linux. |
| VM Insights | VM Insights monitors your Azure VMs. It analyzes the performance and health of your Windows and Linux VMs and identifies their different processes and interconnected dependencies on external processes. The solution includes support for monitoring performance and application dependencies for VMs hosted on-premises or another cloud provider. |
| Network Insights | Network Insights provides a comprehensive and visual representation through topologies, of health and metrics for all deployed network resources, without requiring any configuration. It also provides access to network monitoring capabilities like Connection Monitor, flow logging for network security groups (NSGs), and Traffic Analytics and other diagnostic features. |

Table 7: Summary of Azure Monitor Insights

These specialised Insights should be configured where relevant. VM Insights and Network Insights have been covered in more details in other Core Services designs but will be mentioned here for posterity.

## RBAC

For Azure Monitor the following built-in roles are available[[11]](#footnote-12):

|  |  |
| --- | --- |
| Role Name | Description |
| Monitoring Contributor | Can read all monitoring data and edit monitoring settings. |
| Monitoring Metrics Publisher | Enables publishing metrics against Azure resources |
| Monitoring Reader | Can read all monitoring data (metrics, logs, etc.) |

Table 8: RBAC roles relevant for Azure Monitor

For Azure Application Insights the following RBAC roles are applicable:

|  |  |
| --- | --- |
| Role Name | Description |
| Application Insights Component Contributor | Can edit Application Insights resources. |
| Application Insights Snapshot Debugger | Gives the user permission to use Application Insights Snapshot Debugger features. This role isn't included in the Owner or Contributor roles. |

Table 9: RBAC roles relevant for Azure Application Insights

## 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 Azure Monitor and Insights 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.

### Configuring General Logging and Metrics

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Azure_Monitor_and)

**Design Decision**: AllLogs and allMetrics are configured where applicable to each Azure resource.

**Design Justification**: To troubleshoot and understand infrastructure performance, diagnostic logs and metrics are sent to a central Log Analytics workspace. This has been covered in the Log Analytics Workspace Core Service design document. Any other specific requirements for individual services are covered in the design for that service.

### Configuring VM Insights

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Azure_Monitor_and)

**Design Decision:** The specialised features for VM Insights will be enabled for all Virtual Machines.

**Design Justification:** This has been defined in the Virtual Machine and Managed Disks core service design, but VM Insights will be enabled on all Virtual Machines that support it for more effective diagnosis and troubleshooting capabilities for Virtual Machines which are some of the most critical infrastructure components of the environment.

### Configuring Container Insights

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Azure_Monitor_and)

**Design Decision:** Container Insights should be enabled when there is a use case.

**Design Justification:** Container Insights assist with more effective diagnosis and troubleshooting for issues associated to container-based deployments. Currently there are no use-cases for this service, but it should be considered if modernising to container-based deployments.

### Application Insights

**Design Reference:** Microsoft Security Benchmark [LT-4](#_Azure_Monitor_and)

**Design Decision:** Application Insights will be leveraged.

**Design Justification:** It is assumed that this will be enabled for Platinum, Gold, and Silver applications. It may be enabled for Non-Production or Bronze services if required but is not a mandatory deployment. Specific metrics and application-side configurations should be covered during the Application Landing Zone designs.

### Configuring Network Insights

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

**Design Decision:** Network Insights will be enabled across the platform.

**Design Justification:** It is a requirement to capture networking information, particularly traffic flow. Note that this has already been defined for NSG Flow Logs in the NSG Core Service design. This design decision is for completeness, and to confirm that every subscription should have a specific NetworkWatcher resource in each Azure region.

**Design Details:** Each subscription will have an Azure Network Watcher in each region (two per subscription). There will be one resource group in each subscription that will host the Network Watchers called NetworkWatcher as this is the default resource group deployed when configuring Network Insights.

Each Network Watcher will have the same naming convention: NetworkWatcher\_azureregion.

# Azure Policies

There are no specific Azure Policies required for these services.

# Configuration Templates

## Primary Region Azure Application Insights (Platinum, Gold, Silver)

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| Name | appi-prd-ause-[appname]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia Southeast |
| Resource Mode | Workspace-based |
| Workspace Subscription | AV ALZ Management |
| Workspace Name | log-prd-ause-mgmt-01 |

## Secondary Region Azure Application Insights (Platinum, Gold, Silver)

|  |  |
| --- | --- |
| Configuration Item | Configuration Setting |
| Name | appi-prd-auea-[appname]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Region | Australia East |
| Resource Mode | Workspace-based |
| Workspace Subscription | AV ALZ Management |
| Workspace Name | log-prd-auea-mgmt-01 |

# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://learn.microsoft.com/en-us/azure/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/service-guides/application-insights/operational-excellence [↑](#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/security/benchmark/azure/baselines/azure-monitor-security-baseline [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/azure-monitor/overview [↑](#footnote-ref-9)
9. https://learn.microsoft.com/en-us/azure/azure-monitor/best-practices-data-collection [↑](#footnote-ref-10)
10. https://learn.microsoft.com/en-us/azure/azure-monitor/insights/insights-overview [↑](#footnote-ref-11)
11. https://learn.microsoft.com/en-us/azure/azure-monitor/roles-permissions-security#built-in-monitoring-roles [↑](#footnote-ref-12)