**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 Low Level Design |
| **File Name** | Ambulance Victoria – Azure Monitor and Insights Core Service Low Level Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Draft |
| **Release Date** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Preparation |  |  | |  | |
| **Prepared** | Arshdeep Singh |  | |  | |
| **Authorised** |  | |  | |

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

Table of Contents

[1. Overview 5](#_Toc151034051)

[1.1 Purpose and Audience 5](#_Toc151034052)

[1.2 Scope and Key Deliverables 5](#_Toc151034053)

[1.3 Glossary and Definitions 6](#_Toc151034054)

# Overview

This document covers the low level 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

### Azure Monitor and Insights Operational Excellence Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | 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 |

## RBAC

For Azure Monitor the following built-in roles are available[[2]](#footnote-3):

|  |  |
| --- | --- |
| 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 for Azure Monitor and Insights: -

### 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.

# Configuration Templates for Azure Monitor and Insights:-

## 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 |

Technical and Design recommendations: - (How are we deploying/Doing this)

Azure Monitor and Insights:-

We can use Azure Policy to help enforce the configurations described in the design decisions. Azure Policy allows us to define and enforce rules over Azure resources, including settings related to Azure Monitor and Insights. Here's how we might approach it for each of the design decisions:

1. **Configuring General Logging and Metrics:** We can use Azure Policy to ensure that diagnostic logs and metrics are enabled for each Azure resource. Define a policy that checks if `allLogs` and `allMetrics` are enabled for applicable resources and assign it to each Azure subscriptions or resource groups.

2. **Configuring VM Insights:** For enabling VM Insights on all virtual machines, we can create a policy that checks if VM Insights is enabled and apply it to the virtual machines. Ensure that VM Insights is enabled for all virtual machines that support it.

3. **Configuring Container Insights:** Since Container Insights should be enabled when there is a use case, we might not enforce this with a policy unless we have specific criteria for when Container Insights should be enabled. Instead, consider adding a policy that checks for the presence of use cases and enables Container Insights accordingly.

4. **Application Insights**: Create a policy that ensures Application Insights is enabled for Platinum, Gold, and Silver applications. For Non-Production or Bronze services, we can add a policy that allows enabling Application Insights if required but is not mandatory.

5. **Configuring Network Insights:** Create a policy that checks if Network Insights is enabled across the platform. Ensure that every subscription has a specific NetworkWatcher resource in each Azure region with the specified naming convention.

Configuration Steps:-

To configure Azure Application Insights for Platinum, Gold, and Silver applications in AV Azure environment, we need to follow these steps:

# Primary Region Azure Application Insights

- 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

- 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

We can create these configurations using the Azure portal or Azure Resource Manager templates. Here's a general outline of the steps:

1. Create Log Analytics Workspace:

- Go to the Azure portal and create a new Log Analytics workspace in the specified regions (Australia Southeast and Australia East).

- Note down the workspace IDs and keys for later use.

2. Create Application Insights:

- Go to the Azure portal and create a new Application Insights resource.

- Select the appropriate subscription and resource group.

- Choose the region (Australia Southeast or Australia East) for the primary and secondary regions.

- Select the Log Analytics workspace created earlier as the destination for Application Insights telemetry data.

3. Configure Telemetry:

- In the application's code, configure the Application Insights SDK to send telemetry data to the respective Application Insights resources created above.

4. Verify Configuration:

- Once the configuration is done, verify that telemetry data is being sent to the correct Application Insights resources in both regions.

5. Monitor and Troubleshoot:

- Use the Application Insights portal to monitor and troubleshoot AV applications based on the telemetry data collected.

# Acceptance

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

Data 3 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.

Data3 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 |  |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Data 3 Australia**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. https://learn.microsoft.com/en-us/azure/azure-monitor/roles-permissions-security#built-in-monitoring-roles [↑](#footnote-ref-3)