**CORE SERVICE DESIGN:**

**Log Analytics Workspace**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Log Analytics Workspace Core Service Design |
| **File Name** | Ambulance Victoria – Log Analytics Workspace Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 25/01/2024 |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 25/01/2024 |

Table of Contents

[1. Overview 5](#_Toc157090428)

[1.1 Purpose and Audience 5](#_Toc157090429)

[1.2 Scope and Key Deliverables 5](#_Toc157090430)

[1.3 Glossary and Definitions 6](#_Toc157090431)

[2. Executive Summary 7](#_Toc157090432)

[3. Resource Cost 7](#_Toc157090433)

[4. WAF and Security Control Alignment 9](#_Toc157090434)

[4.1 Reliability 9](#_Toc157090435)

[4.1.1 Overview 9](#_Toc157090436)

[4.1.2 Log Analytics Workspace Reliability Checklist 9](#_Toc157090437)

[4.2 Cost Optimisation 10](#_Toc157090438)

[4.2.1 Overview 10](#_Toc157090439)

[4.2.2 Log Analytics Workspace Cost Optimisation Checklist 10](#_Toc157090440)

[4.3 Operational Excellence 11](#_Toc157090441)

[4.3.1 Overview 11](#_Toc157090442)

[4.3.2 Log Analytics Workspace Operational Excellence Checklist 11](#_Toc157090443)

[4.4 Performance Efficiency 11](#_Toc157090444)

[4.4.1 Overview 11](#_Toc157090445)

[4.4.2 Log Analytics Workspace Performance Efficiency Checklist 11](#_Toc157090446)

[4.5 Security 12](#_Toc157090447)

[4.5.1 Overview 12](#_Toc157090448)

[4.5.2 Log Analytics Workspace Security Checklist 12](#_Toc157090449)

[Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate intrusion and/or compromise of data. 13](#_Toc157090450)

[5. Architecture Summary 14](#_Toc157090451)

[5.1 Resource Overview 14](#_Toc157090452)

[5.2 RBAC 14](#_Toc157090453)

[5.3 Solution Diagram 15](#_Toc157090454)

[5.4 Design Decisions and Justifications 16](#_Toc157090455)

[5.4.1 Number and Location of Log Analytics Workspaces 16](#_Toc157090456)

[5.4.2 Logging and Monitoring 16](#_Toc157090457)

[5.4.3 Data Retention Period 16](#_Toc157090458)

[6. Azure Policies 17](#_Toc157090459)

[7. Configuration Templates 19](#_Toc157090460)

[7.1 Primary Region Central Log Analytics Workspace 19](#_Toc157090461)

[7.2 SecondaryRegion Central Log Analytics Workspace 19](#_Toc157090462)

[7.3 Generic Primary Region Central Log Analytics Workspace 19](#_Toc157090463)

[7.4 Generic DR Region Central Log Analytics Workspace 20](#_Toc157090464)

[8. Acceptance 21](#_Toc157090465)

# Overview

This document covers the baseline design for the Log Analytics Workspace 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 Log Analytics Workspace 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 Log Analytics Workspace.

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 Log Analytics Workspace 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 |
| **LAW** | Log Analytics Workspace |

Table 1: Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Log Analytics Workspace 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 Cost Optimisation and Security were relevant.

For this service the main baseline configurations include:

* One primary Log Analytics Workspace will be created in each region and hosted in the AV ALZ Management subscription.
* A Sentinel specific Log Analytics Workspace will be created under the AV ALZ Security subscription.
* All resources within a region that require log collection will send their logs to the primary Log Analytics Workspace for that region.
* The Log Retention period will be set to 90 days.
* If an Application Landing Zone requires its own Log Analytics Workspace it may be created in accordance with the Configuration Templates provided in this document.

# Resource Cost

The base costing for Log Analytics Workspace is shown below. The pricing varies based on the number of logs ingested and the retention periods set[[2]](#footnote-3).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Plan | Capabilities | Pricing Tier | Price | Effective Per GB Price1 | Savings Over Pay-As-You-Go |
| Basic Logs | * 8 days included interactive retention * Log search2 queries * Up to 12 years data archive2 | Pay-As-You-Go | **$1.022** /GB | **$1.022** /GB | N/A |
| Analytics Logs | * 30/90\* days included interactive retention * All queries supported enabling powerful analytics * Out-of-the-box monitoring insights built on analytic logs * Supports workbooks and dashboards * Up to 2 years interactive retention2 * Up to 12 years archive2 * Alerting2 | Pay-As-You-Go | **$4.877** /GB | **$4.877** /GB | N/A |
| 100 GB per day | **$400.62** /day | **$4.01** /GB | 18% |
| 200 GB per day | **$752.18** /day | **$3.77** /GB | 23% |
| 300 GB per day | **$1,103.74** /day | **$3.68** /GB | 25% |
| 400 GB per day | **$1,438.94** /day | **$3.60** /GB | 26% |
| 500 GB per day | **$1,768.02** /day | **$3.54** /GB | 27% |
| 1,000 GB per day | **$3,474.71** /day | **$3.48** /GB | 29% |
| 2,000 GB per day | **$6,785.90** /day | **$3.40** /GB | 30% |
| 5,000 GB per day | **$16,453.76** /day | **$3.30** /GB | 33% |
| 10,000 GB per day | **$31,967.30** /day | **$3.20** /GB | 34% |
| 25,000 GB per day | **$77,567.71** /day | **$3.11** /GB | 36% |
| 50,000 GB per day | **$150,434.34** /day | **$3.01** /GB | 38% |

Table 2: Baseline pricing construct

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Log Analytics Workspace Reliability Checklist

There is no guidance for Log Analytics Workspace under the Reliability pillar.

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[4]](#footnote-5). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Log Analytics Workspace Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Consider adoption of the Commitment Tiers pricing model to the Log Analytics workspace. | Yes | No | Governance | Operational – review monthly |
| **CO2** | Evaluate daily cap usage to limit the daily ingestion for your workspace. | Yes | No | Governance | Operational – review monthly |
| **CO3** | Understand Log Analytics workspace usage. | Yes | No | Governance | Operational |
| **CO4** | Evaluate possible data ingestion volume reducing. | Yes | No | Governance | Operational – review quarterly |

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

### Log Analytics Workspace Operational Excellence Checklist

There is no guidance for Log Analytics Workspaces under the Operational Excellence pillar.

## 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

### Log Analytics Workspace Performance Efficiency Checklist

There is no guidance for Log Analytics Workspace under the Performance Efficiency pillar.

## 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.

### Log Analytics Workspace Security Checklist

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | DH Ref. | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **S1** | 16.1.1 | Establish and maintain an audit log management and monitoring process that defines the enterprise’s logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Yes | No | Governance | Operational – review quarterly |
| **S2** | 16.2.1 | Collect audit logs and ensure adequate audit log storage for critical servers, workstations, laptops and other devices and stored securely. | Yes | Yes | IaC | At deployment of each resource |
| **S3** | 16.2.4 | Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events. | Yes | Yes | IaC | At deployment |
| **S4** | 16.3.1 | Centralize, to the extent possible, audit log collection and retention across enterprise assets. | Yes | Yes | IaC | At deployment |
| **S5** | 16.3.2 | Retain audit logs across enterprise assets for a minimum of 90 days. | Yes | Yes | IaC | At deployment |
| **S6** | 16.3.3 | Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis. | Yes | No | Governance | Operational – review weekly |
| **S7** | 16.3.4 | Continuously monitor inbound and outbound network traffic to identify unusual activity or trends that could indicate intrusion and/or compromise of data. | Yes | No | Sentinel | Operational – review and respond to Sentinel alerts frequently |

Table 4: Security checklist summary

# Architecture Summary

## Resource Overview

Log Analytics Workspace is an analysis tool that allows log data from Azure Monitor and other services be queried and searched[[7]](#footnote-8).

## RBAC

The following roles are applicable for this resource:

|  |  |
| --- | --- |
| Role Name | Description |
| Log Analytics Contributor | Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; reading storage account keys to be able to configure collection of logs from Azure Storage; adding solutions; and configuring Azure diagnostics on all Azure resources. |
| Log Analytics Reader | Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azure diagnostics on all Azure resources. |
| Data Purger | Delete private data from a Log Analytics workspace. |

Table 5: RBAC roles relevant for this core service

## Solution Diagram



Figure 1: Log Analytics Workspace Centralised configuration

## 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 Log Analytics Workspace 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.

### Number and Location of Log Analytics Workspaces

**Design Reference:** Table 6 – [S4](#_Log_Analytics_Workspace)

**Design Decision**: A central Log Analytics Workspace will be deployed in each region in the AV ALZ Management Subscription. A separate instance of Log Analytics Workspace will be used for Microsoft Sentinel.

**Design Justification**: Security and simplicity of management principals suggest the best way to deploy Log Analytics Workspaces is to centralise the collection of logs as much as possible. Only one Log Analytics solution can be deployed per region, so it is recommended to have two central workspaces – one in each Azure region. For specific applications such as Azure Sentinel another workspace will be deployed to provide segregation of the Sentinel data as compared to general logs and diagnostics.

### Logging and Monitoring

**Design Reference:** Table 6 – [S2, S3](#_Log_Analytics_Workspace)

**Design Decision:** diagnostic settings will be enabled for the Log Analytics Workspace itself. All other resources will send their diagnostic logs to the central Log Analytics Workspace in that region. AllLogs and allMetrics will be captured for the Log Analytics Workspace diagnostic setting.

**Design Justification:** All resources, including the Log Analytics Workspace itself, must have their logs captured and stored as centrally as possible so that they can be reviewed for suspicious activity or operational optimisation purposes. There will be one central Log Analytics Workspace per region, so all resources will send their logs to the workspace in its respective region.

### Data Retention Period

**Design Reference:** Table 6 – [S5](#_Log_Analytics_Workspace)

**Design Decision:** the retention period will be set at 90 days.

**Design Justification:** It is a compliance requirement stipulated by the Department of Health controls that logs will be retained for a minimum of 90 days.

### Daily Cap Limit

**Design reference:** Table 3 – [CO2](#_Log_Analytics_Workspace_1)

**Design Decision:** A daily cap limit of 100GB will be set.

**Design Justification:** The daily cap limit assists in cost management of log analytics workspace. The 100GB will be the initial cap set as the current daily ingestion at the time of writing is approximately 10GB, and at 100GB the first discount tier can be set. Over time the ingestion is expected to increase as more applications are brought online, so the new pricing tier should be set once an average of 100GB per day is reached.

# Azure Policies

Though this policy does not specifically apply to the Log Analytics Workspace, it sets diagnostic settings for all resources in that region through Azure Policy so that they do not need to be coded or applied at deployment each time.

|  |  |
| --- | --- |
| Policy Name | Scope |
| Deploy-Resource-Diag-Australia-Southeast | av management group (under Root) |
| Deploy-Resource-Diag-Australia-East | av management group (under Root) |

Table 6: Azure Policies

Note that for any resources not listed, thought the IaC templates will have the capability to deploy them, it is also best to add that resource into the policies above so that this can be done by Policy and reduce the dependency on having this defined in IaC templates. The following resources are included in the above policies:

* NSG
* Public IP
* Application Gateway
* Time Series Insights
* Cognitive Services
* Data Lake Analytics
* Virtual Machines
* Azure Data Explorer Cluster
* App Service
* Event Grid System Topic
* Virtual Network
* Analysis Services
* SQL Elastic Pools
* Stream Analytics
* Power BI Embedded
* Event Grid Topic
* Traffic Manager
* Search Services
* Azure Data Lake Store
* Storage Accounts
* ExpressRoute
* Load Balancer
* CDN Endpoint
* Logic Apps
* Event Grid Subscriptions
* Network Interfaces
* ML Workspaces
* Logic Apps
* Data Factory
* Azure Function App
* WVD
* PostgreSQL
* Service Bus
* App Service Plan
* Automation Accounts
* Databricks
* Redis Cache
* Azure Media Service
* Front Door
* HD Insight
* Key Vault
* Firewall
* Event Hubs
* Azure API for FHIR
* APIM
* MariaDB
* SignalR
* Cosmos DB
* VPN Gateway
* SQL DB
* IOT
* MySQL DB
* Virtual Machines Scale Sets
* SQL Managed Instances
* Container Registry
* Kubernetes
* Container Instances

# Configuration Templates

## Primary Region Central Log Analytics Workspace

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| Name | log-prd-ause-mgmt-01 |
| Subscription | AV ALZ Management |
| Resource Group | rg-prd-ause-management-01 |
| Pricing Tier | Pay-as-you-go |
| Data Retention | 90 days |
| Diagnostic Settings to be captured | allLogs  AllMetrics |
| Log Analytics Workspace for logs | log-prd-ause-mgmt-01 |

## SecondaryRegion Central Log Analytics Workspace

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| Name | log-prd-auea-mgmt-01 |
| Subscription | AV ALZ Management |
| Resource Group | rg-prd-auea-management-01 |
| Pricing Tier | Pay-as-you-go |
| Data Retention | 90 days |
| Diagnostic Settings to be captured | allLogs  AllMetrics |
| Log Analytics Workspace for logs | log-prd-auea-mgmt-01 |

## Generic Primary Region Central Log Analytics Workspace

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| Name | log-[env]-ause-[appname]-[workload]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Pricing Tier | Pay-as-you-go |
| Data Retention | 90 days |
| Diagnostic Settings to be captured | allLogs  AllMetrics |
| Log Analytics Workspace for logs | log-prd-ause-mgmt-01 |

## Generic DR Region Central Log Analytics Workspace

|  |  |
| --- | --- |
| Configuration Item | Configuration Value |
| Name | log-[env]-auea-[appname]-[workload]-01 |
| Subscription | AV ALZ [Subscription Name] |
| Pricing Tier | Pay-as-you-go |
| Data Retention | 90 days |
| Diagnostic Settings to be captured | allLogs  AllMetrics |
| Log Analytics Workspace for logs | 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://azure.microsoft.com/en-us/pricing/details/monitor/ [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview [↑](#footnote-ref-8)