**CORE SERVICE DESIGN:**

**Log Analytics Workspace Low Level Design**

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 Low Level Design |
| **File Name** | Ambulance Victoria – Log Analytics Workspace Low Level Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Review |
| **Release Date** |  |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 30/04/2024 |

Table of Contents

[1. Overview 5](#_Toc167375286)

[1.1 Purpose and Audience 5](#_Toc167375287)

[1.2 Scope and Key Deliverables 5](#_Toc167375288)

[1.3 Glossary and Definitions 5](#_Toc167375289)

[2. Executive Summary 7](#_Toc167375290)

[3. Resource Cost 7](#_Toc167375291)

[4. Architecture Summary 8](#_Toc167375292)

[4.1 Resource Overview 8](#_Toc167375293)

[4.2 RBAC 8](#_Toc167375294)

[4.3 Solution Diagram 9](#_Toc167375295)

[4.4 Design Decisions and Justifications 10](#_Toc167375296)

[4.4.1 Number and Location of Log Analytics Workspaces 10](#_Toc167375297)

[4.4.2 Logging and Monitoring 10](#_Toc167375298)

[4.4.3 Security Logging:- 10](#_Toc167375299)

[4.4.4 Data Retention Period 11](#_Toc167375300)

[4.4.5 Daily Cap Limit 11](#_Toc167375301)

[4.4.6 DH Platform Logging 11](#_Toc167375302)

[5. Azure Policies 13](#_Toc167375303)

[5.1 Diagnostic Settings 13](#_Toc167375304)

[5.2 Azure Policy for Activity Logs going to Event Hub 16](#_Toc167375305)

[5.3 Azure Policy for Sentinel 16](#_Toc167375306)

[6. Configuration Templates 17](#_Toc167375307)

[6.1 Primary Region Central Log Analytics Workspace 17](#_Toc167375308)

[6.2 SecondaryRegion Central Log Analytics Workspace 17](#_Toc167375309)

[6.3 Generic Primary Region Central Log Analytics Workspace 17](#_Toc167375310)

[6.4 Generic DR Region Central Log Analytics Workspace 18](#_Toc167375311)

[6.5 Logging Standards 18](#_Toc167375312)

[6.6 Data Sources 18](#_Toc167375313)

[7. Acceptance 19](#_Toc167375314)

# Overview

This document provides a detailed low-level design for the Log Analytics Workspace (LAW) in the context of Ambulance Victoria's Azure tenancy. The LAW is a critical component for centralized log collection, analysis, and monitoring of Azure resources and services. This design aims to ensure a robust and scalable LAW implementation aligned with best practices and security standards.

The design covers various aspects of LAW configuration, including data collection rules, retention policies, data sources, and access control. It also includes recommendations for integrating LAW with other Azure services and monitoring tools to enhance visibility and operational efficiency.

By following this low-level design, we can effectively utilize the LAW to gain valuable insights, troubleshoot issues, and ensure compliance with regulatory requirements.

## Purpose and Audience

This document provides the detailed design and configuration of Azure Log Analytics Workspace in Ambulance Victoria’s Azure tenancy. It serves as a Low-Level Design from an architectural perspective, outlining the configuration items, enabling instructions, for Log Analytics Workspace.

The audience for this document is those involved in the planning, designing, and implementing of the Log Analytics Workspace. 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 low-level design and implementations for the Log Analytics Workspace Low Level Design.

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

The Log Analytics Workspace (LAW) Low Level Design adheres to the baseline standards set by the Microsoft Well-Architected Framework (WAF) and the Department of Health Security Controls. This summary highlights the key design decisions made for LAW deployment, focusing on cost optimization and security.

Key Baseline Configurations:

* Primary LAW in Each Region: One primary LAW will be created in each region, hosted in the AV ALZ Management subscription.
* Sentinel Specific LAW: A separate LAW will be created under the AV ALZ Security subscription for Sentinel.
* Centralized Log Collection: All resources within a region requiring log collection will send their logs to the primary LAW for that region.
* Log Retention Period: The log retention period will be set to 90 days.
* Custom LAW Creation: Application Landing Zones requiring their own LAW may be created following the Configuration Templates provided in this document.

These configurations ensure a standardized approach to LAW deployment, meeting the requirements of both WAF and Department of Health Security Controls.

# 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[[1]](#footnote-2).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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

# 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[[2]](#footnote-3).

## RBAC

The Log Analytics Workspace (LAW) implements Role-Based Access Control (RBAC) to manage access to its resources. The following roles are applicable for the LAW:

1. **Log Analytics Contributor:**

Description: 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 configure collection of logs from Azure Storage; adding solutions; and configuring Azure diagnostics on all Azure resources.

Permissions: Read and edit monitoring data and settings.

2. **Log Analytics Reader:**

Description: Log Analytics Reader can view and search all monitoring data as well as view monitoring settings, including viewing the configuration of Azure diagnostics on all Azure resources.

Permissions: View and search monitoring data and settings.

3. **Data Purger:**

Description: Data Purger role allows users to delete private data from a Log Analytics workspace.

Permissions: Delete private data from the workspace.

Assign these roles to users and groups based on the principle of least privilege, ensuring that individuals have only the permissions necessary to perform their job functions. Regularly review and audit role assignments to maintain security and compliance.

## Solution Diagram



Figure 1: Log Analytics Workspace Centralised configuration

## Design Decisions and Justifications

This section outlines the key design decisions and justifications for the Log Analytics Workspace (LAW) Low-Level Design core service based on the findings of the WAF and Security alignment.

### Number and Location of Log Analytics Workspaces

* **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:** Centralizing log collection simplifies management and enhances security. Deploying one workspace per region ensures regional coverage. Using a separate workspace for Microsoft Sentinel segregates its data from general logs and diagnostics.

### Logging and Monitoring

* **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:** Centralized logging enables effective monitoring and analysis. Capturing AllLogs and allMetrics ensures comprehensive monitoring of all resources, including the Log Analytics Workspace.

### Security Logging:-

* **Design Decision:** There are 2 destinations for security logs.

**1 DH SOC Security Logs Destination**

* 1. **Source: - Subscription level Activity Logs**

**Destination**: Event Hub -> Open Collector -> DH SOC's SIEM (Log Rhythm)

**Configuration:** Configure these logs to send to Event Hub and from Event Hub to IPSEC Open Collector.

Configure the Log Analytics Workspace to send security logs to an Event Hub. Configure the Event Hub to forward logs to the Log Rhythm Collector. Ensure that the Log Rhythm Open Collector is configured to receive logs from the Event Hub.

* 1. **Source: - System Security Logs**

**Destination**: Event Hub -> Collector -> DH SOC's SIEM (Log Rhythm)

**Configuration:** Configure these logs to send to Event Hub and from Event Hub to IPSEC Collector.

**2 Sentinel Security Logs Destination**

**Destination:** Azure Sentinel

**Configuration**: Configure the Log Analytics Workspace to send security logs to Azure Sentinel. This will allow AV's own SIEM to capture the same security logs.

### Data Retention Period

* **Design Decision:** The retention period will be set at 90 days.
* **Design Justification:** A minimum 90-day retention period is mandated by the Department of Health controls for compliance and auditing purposes.

### Daily Cap Limit

* **Design Decision:** A daily cap limit of 100GB will be set.
* **Design Justification:** Setting a daily cap limit helps manage costs. The initial 100GB cap aligns with current ingestion rates, enabling qualification for the first discount tier. As ingestion rates increase over time, the pricing tier will be adjusted accordingly.

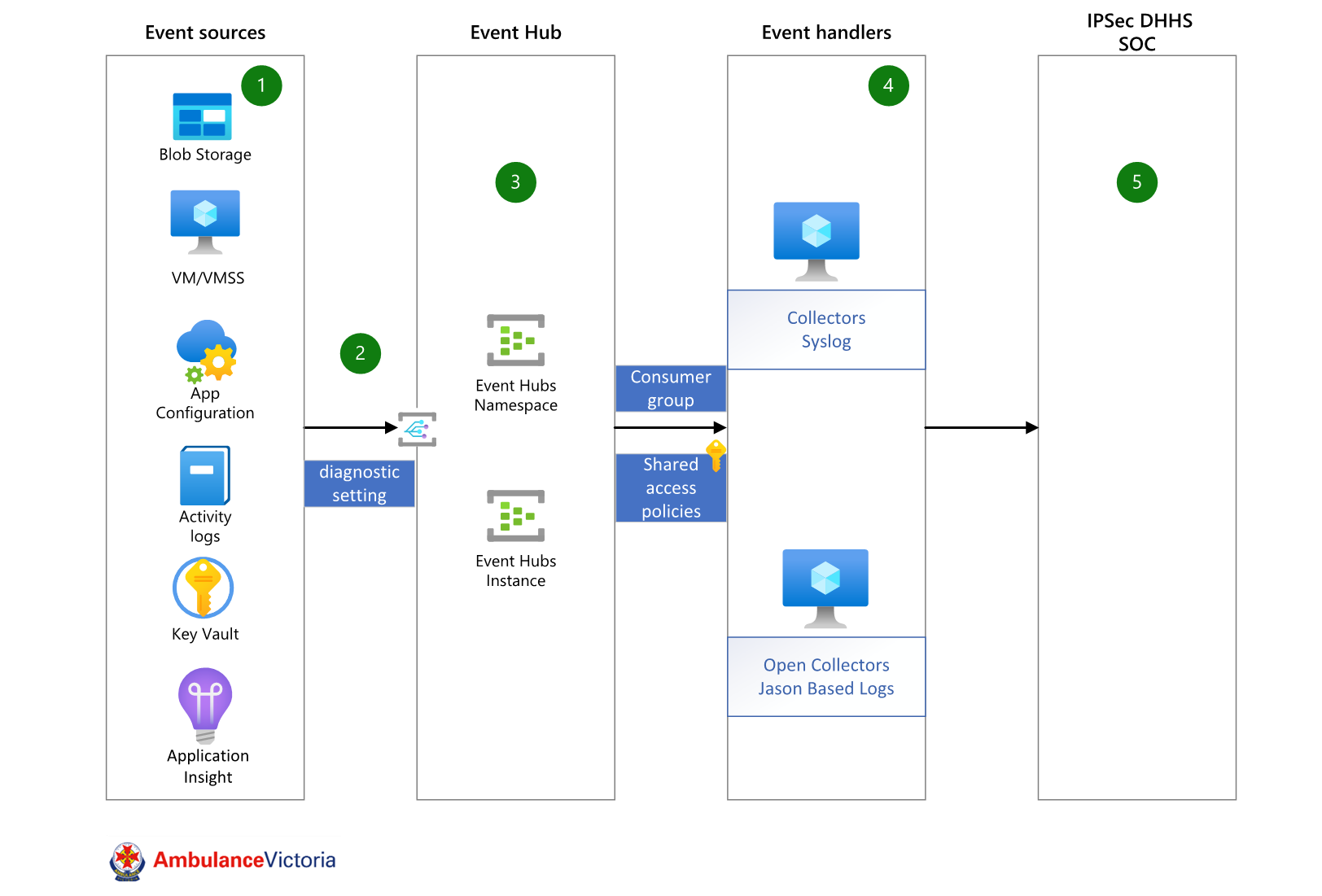
### DH Platform Logging

As per above we will be having 3 Log Analytics workspaces, one centralized workspace in each region under AV ALZ Management subscription and one under AV ALZ Security Subscription for Azure Sentinel. Diagnostic settings will be enabled all workspaces to collected activity and security logs.

Now for Department of Health we have a specific requirement to forward the activity and security logs to their Log Rhythm. To achieve that we will have all the logs stream to Event Hub from which it will be passed on to IPSec (which is DH external vendor) Collectors which then will ingest the logs to the DH Log Rhythm system.

For AV context, we will have the AV Sentinel Log Analytics Workspace set up to forward the logs to SysLog Server which will ingest the logs to AV Sentinel.

Here is a diagram showing log flow for DH Logging Requirements.



**Collectors:** LogRhythm System Monitor Agents (Collectors) are typically installed on one or more Windows Server virtual machines. IPSec SOC’s recommendations for where and how to deploy collectors are as follows: • At least one dedicated agent per each major site. If the site is critical, two collectors are recommended • If a site has low WAN bandwidth and a reasonable number of log sources, deploy a collector locally • In some circumstances, a collector can be deployed to collect logs from a non-domain joined host or DMZ host. Speak with your SIEM Security Engineer for details. A collector will either reach out to hosts and pull logs in via MS Events, UDLA connections, making API calls, or via reading a log file. A collector also functions as a syslog server to receive syslog data from networking devices such as switches, firewalls, security devices etc.

**Open Collectors**: are typically installed on a virtual machine running CentOS 7. The Open Collector brings modern logs, usually in JSON format, from cloud log sources, flat file, or other formats, into the LogRhythm SIEM. It is designed for easy mapping of JSON fields to the LogRhythm Schema. The Open Collector uses Elastic Beats to grab the data from the device and pass it along to the Open Collector, where the normalization takes place. Eventually, the System Monitor Agent will do only what the name implies—monitor a single system. LogRhythm is beginning the transition to Open Collector with popular logs for which the Open Collector's JSON-native log capabilities add a lot of value. This includes AWS, O365, and JSON logs that come in over flat file or syslog.

# Azure Policies

# 5.1 Diagnostic Settings

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) |

Below policies Initiatives are already deployed that ensures that diagnostics settings are enabled for all resources in both the regions.

Logs are pointed to the log analytics workspaces: -

law-prd-ause-mgmt-01 and law-prd-auea-mgmt-01

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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

# 5.2 Azure Policy for Activity Logs going to Event Hub

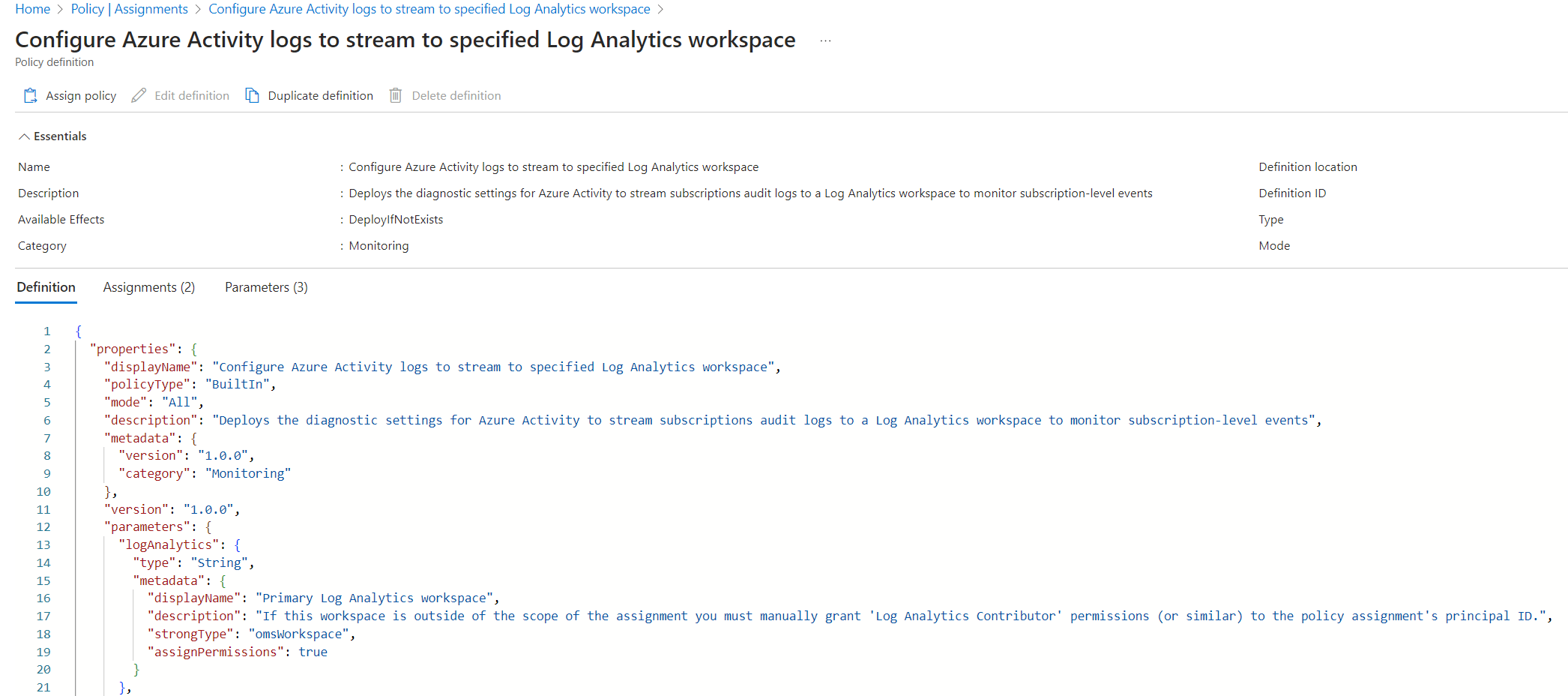
In addition to above below Azure policy can be used to stream the subscription level activity logs to a specified event hub. There are 2 ways, First using log profile to export activity log events to event hubs. Second, using a custom policy: -

Details of both these methods are provided under MS build topics link below: -

[Policy to stream subscription level logs to an event hub - Microsoft Q&A](https://learn.microsoft.com/en-us/answers/questions/1183625/policy-to-stream-subscription-level-logs-to-an-eve)

# 5.3 Azure Policy for Sentinel

We can use below Azure policy to stream activity logs to AV Sentinel Workspace.



# 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 |

## Logging Standards

Retention: -

|  |  |  |  |
| --- | --- | --- | --- |
| Log Types | Subscription | Log Analytics Workspace | Retention |
| Security Logs & Events | Security | [law-prd-ause-sentinel-01](https://portal.azure.com/#@AmbulanceVic.onmicrosoft.com/resource/subscriptions/f8a25f49-4ff7-4e29-b6b9-2094fcd799bf/resourceGroups/rg-prd-ause-sentinel-01/providers/Microsoft.OperationalInsights/workspaces/law-prd-ause-sentinel-01) | 12months  + 24 months Archive |
| All other Logs, Events & Performance Metrics | Management | [law-prd-ause-mgmt-01](https://portal.azure.com/#@AmbulanceVic.onmicrosoft.com/resource/subscriptions/5f0b73f8-677f-4746-987f-3661992e7f9b/resourceGroups/rg-prd-ause-management-01/providers/Microsoft.OperationalInsights/workspaces/law-prd-ause-mgmt-01) | 90days + 24 months Archive |

## Data Sources

|  |  |  |
| --- | --- | --- |
| **Data Source** | **Event Type** | **Log Analytics Workspace** |
| Windows Event Logs | Application | Management |
|  | System | Management |
|  | Security | Security (Sentinel) |
| Syslog | AV | Sentinel Log Analytics |
|  | DH | Sys Log Server |
| Performance Counters | CPU | Management |
|  | Memory | Management |
|  | Disk | Management |
|  | Network | Management |
| Defender for Cloud | AV | Security (Sentinel) |
| Defender for Servers | AV | Security (Sentinel) |
| Network Device Syslog | Activity | Syslog Server |
| Azure Firewall | Audit Logs | Security (Sentinel) |
| NSGs | Flow Logging | Security (Sentinel) |

# 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 Data3 Australia**

|  |  |
| --- | --- |
| Name | Arshdeep Singh |
| Position | Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://azure.microsoft.com/en-us/pricing/details/monitor/ [↑](#footnote-ref-2)
2. https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview [↑](#footnote-ref-3)