**Azure Monitor, Insights and Alerting Combined Low-Level Design**

atabricks

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

|  |  |
| --- | --- |
| Document Control | |
| **Template Version** | Created from Template 2024.01 |
| **Title** | **Azure Monitor, Insights and Alerting Low-Level Design Document** |
| **File Name** | **Azure Monitor, Insights and Alerting Low-Level Design Document** |
| **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 | 26/04/2024 |

Table of Contents

[1. Overview 6](#_Toc165027274)

[1.1 Purpose and Audience 6](#_Toc165027275)

[1.2 Scope and Key Deliverables 6](#_Toc165027276)

[1.3 Glossary and Definitions 7](#_Toc165027277)

[2. Executive Summary 7](#_Toc165027278)

[3. Architecture 8](#_Toc165027279)

[3.1 Solution Diagram for Azure Monitor 8](#_Toc165027280)

[3.2 Solution Diagram for Azure Alerts 8](#_Toc165027281)

[4. Azure Monitor Cost 9](#_Toc165027282)

[5. Azure Monitor Solution 10](#_Toc165027283)

[5.1 Azure Alert Implementation 10](#_Toc165027284)

[5.2 Azure Monitor Logs Implementation 11](#_Toc165027285)

[5.3 Azure Service Health Implementation 11](#_Toc165027286)

[5.4 Azure Monitor Workbooks Implementation 11](#_Toc165027287)

[5.5 Azure Activity Log Implementation 11](#_Toc165027288)

[5.6 Azure Resource Health Alerts Implementation 11](#_Toc165027289)

[5.7 Configure Metric Alerts 11](#_Toc165027290)

[6. Azure Monitor Insights solution 12](#_Toc165027291)

[6.1 Application Insight Configuration 12](#_Toc165027292)

[6.2 Data Collection Rules (DCR) Configuration 12](#_Toc165027293)

[6.3 Data Collection Rules (DCR) Automation 12](#_Toc165027294)

[7. Governance 12](#_Toc165027295)

[7.1 Diagnostic Settings Configuration 12](#_Toc165027296)

[7.2 Monitoring Application with Application Insight 12](#_Toc165027297)

[7.3 Monitoring VM with VM Insight 13](#_Toc165027298)

[7.4 Monitoring Container with Container Insight 13](#_Toc165027299)

[7.5 Monitoring Network with Network Insight 13](#_Toc165027300)

[7.6 Monitoring Storage Account with Storage Insight 13](#_Toc165027301)

[7.7 Monitoring Key Vault with Key Vault Insight 13](#_Toc165027302)

[8. Operations 14](#_Toc165027303)

[8.1 VM Monitoring Deployment Agent 14](#_Toc165027304)

[8.2 Storage Account Monitoring Enforcement 14](#_Toc165027305)

[8.3 Key Vault Monitoring Deployment Agent 14](#_Toc165027306)

[9. Azure Monitor Access Control 15](#_Toc165027307)

[9.1 Overview 15](#_Toc165027308)

[9.2 Built-In Monitoring Roles 15](#_Toc165027309)

[9.3 Assignments 15](#_Toc165027310)

[9.4 Implementation Steps 15](#_Toc165027311)

[10. Azure Monitor Security Control 16](#_Toc165027312)

[10.1 Implementation Steps 16](#_Toc165027313)

[11. Configuration Templates for Azure Alerts:- 17](#_Toc165027314)

[11.1 Service Health Alert Settings 17](#_Toc165027315)

[11.2 Resource Health Alert Settings 19](#_Toc165027316)

[11.3 Microsoft Entra Alert Settings 21](#_Toc165027317)

[11.4 Metric Alert Settings 22](#_Toc165027318)

[11.4.1 Azure Application Gateway 22](#_Toc165027319)

[11.4.2 Azure Virtual Machines 22](#_Toc165027320)

[11.4.3 Storage Accounts 24](#_Toc165027321)

[11.4.4 Log Analytics 25](#_Toc165027322)

[Configuration Templates for Azure Monitor and Insights: - 25](#_Toc165027323)

[11.5 Primary Region Azure Application Insights (Platinum, Gold, Silver) 25](#_Toc165027324)

[11.6 Secondary Region Azure Application Insights (Platinum, Gold, Silver) 26](#_Toc165027325)

[Acceptance 26](#_Toc165027326)

# Overview

Ambulance Victoria's digital transformation initiative is a strategic Endeavor aimed at modernizing its operations and services through the adoption of digital technologies. As part of this transformation, Ambulance Victoria is evaluating a Datacenter exit strategy, which involves transitioning its IT infrastructure and services away from traditional on-premises datacentres to cloud-based solutions or other modern hosting platforms.

Key Components of the Digital Transformation and Datacenter Exit Strategy:

1. Cloud Adoption
2. Datacenter Exit
3. Infrastructure and Application Modernisation

To facilitate an Enterprise Infrastructure platform to support Ambulance Victoria’s digital transformation, A well architected Azure Tenant is configured that requires the need for enabling Key Azure services like Azure Monitor, Azure Alerts and other Azure platform services.

## Purpose and Audience

This document provides the detailed design and configuration of Azure Monitor, Insights, and Alerting in Ambulance Victoria’s Azure tenancy. It serves as a Low-Level Design from an architectural perspective, outlining the configuration items, enabling instructions, and centralized monitoring and management platforms for Azure resources and services health.

The purpose of this document is to:

* Provide an overview of Azure Monitor's configuration items.
* Instruct on enabling and configuring the necessary items.
* Establish a centralized platform for monitoring and managing Azure resource performance.
* Establish a centralized platform for monitoring and managing Azure services health.

The audience for this document is those involved in the planning, designing, and implementing of the Azure Monitor, Insights, and Alerting 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 design document encompasses the architecture and configuration of Azure Monitor, focusing on the following aspects:

* + Azure Monitor Configurations
  + Azure Monitor Logs and associated Log Analytics Workspace
  + Workbooks related to Azure Monitor
* Azure Monitor Insights
* Azure Alerting
* Recommendations of IaC templates for Azure Resources with insight capabilities.

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **VMSS** | Virtual Machine Scale Set |
| **VNet** | Virtual Network |
| **RT** | Route Table |
| **RBAC** | Role Based Access Control |
| **LB** | Load Balancer |
| **AKS** | Azure Kubernetes |
| **IaaS** | Infrastructure as a Service |
| **WAF** | Web Application Firewall |
| **LAW** | Log Analytics Workspace |

# Executive Summary

Azure Monitor is a comprehensive monitoring service provided by Microsoft Azure, designed to help organizations gain insights into the performance and health of their applications, infrastructure, and networks running on the Azure cloud platform. It offers a range of features for monitoring, collecting, analysing, and acting on telemetry data from various sources, including applications, virtual machines, containers, and more.

This design also covers the baseline standards for the Azure Alerts. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

# Architecture

## Solution Diagram for Azure Monitor

A computer screen shot of a diagram

Description automatically generated

## Solution Diagram for Azure Alerts

**A screenshot of a computer

Description automatically generated**

# Azure Monitor Cost

While Azure Monitor itself doesn’t have a direct cost, utilizing its capabilities for monitoring, logging, and analysing telemetry data from various Azure services and resources incurs specific pricing based on usage:

Metrics

Azure Monitor does not cost anything for collecting and storing basic metrics data. However, there are costs associated with custom metrics or extended data retention.

Logs

Azure Monitor Logs collect and analyse log data from Azure resources, applications, and custom sources. The cost is based on the volume of data ingested and stored.

Alerts

Alerts based on metrics and logs are a basic functionality of Azure Monitor and do not incur additional costs. However, forwarding alerts to external services like Splunk or AWS Workspace may have extra costs.

Application Insights

Integrated with Azure Monitor, Application Insights provides application performance monitoring (APM) capabilities. The cost is based on the volume of telemetry data collected and stored.

Network Monitoring

Network monitoring in Azure Monitor shows telemetry of performance and connectivity of virtual networks, VPN gateways, and ExpressRoute circuits. There are no costs associated with network monitoring.

Service Health

Azure Monitor provides insights into the health and availability of Azure services at no extra cost.

Pricing for Various Alert Types

The following pricing applies to various alert types:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Alert Type | Free units included | Alert rule price (Monthly) | Time Series Price (Monthly) | Additional cost for metric alert w/ dynamic threshold14 |
| Activity Log Alert | Limited to 100 rules per subscription | N/A | N/A | N/A |
| Native Metrics11, 12 | 10 monitored metric time-series per month13 | N/A | **$0.153** | **$0.153** |
| Log Alert (15 minute frequency) | First time-series is included in the log alert rule | **$0.764** | **$0.077** | N/A |
| Log Alert (10 minute frequency) | First time-series is included in the log alert rule | **$1.528** | **$0.153** | N/A |
| Log Alert (5 minute frequency) | First time-series is included in the log alert rule | **$2.292** | **$0.230** | N/A |
| Log Alert (1 minute frequency) | First time-series is included in the log alert rule | **$4.583** | **$0.459** | N/A |

# Azure Monitor Solution

Here is a low-level Azure Monitor and Alerting Solution Design.

# 5.1 Azure Alert Implementation

**Action Groups Setup:**

Create below Action Groups at each Landing Zone Level:

1. Infrastructure Alert Group for Infrastructure Operations with Email notification.

2. Application Alert Group for Application Operations with Email notification.

3. Security Alert Group for Security Operations with Email notification.

4. Landing Zone Cost Alert for Platform Owner and Application Owner with Email notification.

5. Network Alert group for Network Operations with Email notifications.

6. IDAM Alert Group for Identity and Access Management Team with same email notifications.

Alert Action Groups details as below:-

ag-infra-01

ag-network-01

ag-security-01

ag-database-01

**Signal Measures Baseline:**

Set Signal Measures to "All Administrative Operations".

**Alert Rules Configuration:**

Metric alert rules for Availability, Performance, and Security.

Event Level selected for "Warning", "Error", "Critical", "Informational" for resource level alerts.

All Event Status (Failed, Started, succeeded) selected for resource level alerts.

# 5.2 Azure Monitor Logs Implementation

**Data Collection Rules:**

Set up data log collection rules for monitored Azure resources.

**Application Log Analytics Workspace:**

Create an Application Log Analytics Workspace.

**Alerting & Monitoring Configuration:**

Configure alerting and monitoring based on Logs data.

# 5.3 Azure Service Health Implementation

**Service Health Notifications:**

* Create Azure Services Health notifications for Planned Maintenance, Health, and Security Advisories for Australia East and Australia Southeast regions. This need to be done for each subscription.

# 5.4 Azure Monitor Workbooks Implementation

**Default Workbooks Usage:**

* Security Operations team should use default workbooks like Azure Resources Locations, Storage Account Overview, and Key Vault Overview for specific insights analysis via dashboards.

# 5.5 Azure Activity Log Implementation

**Usage for Auditing and Compliance:**

* Use Azure Activity Log for auditing and transfer azure activity log to the log analytics workspace (find the law name).

**Log Transfer to Log Rhythm:**

* Configure central log analytics workspace to forward all Activity Logs in Azure Monitor to be transferred to Log Rhythm for monitoring.

# 5.6 Azure Resource Health Alerts Implementation

* Create Resource Health Alerts for all resource types in each subscription.
* Set alerts to include all future resource groups.

## Configure Metric Alerts

* Configure metric alert rules for major resources.
* Use static thresholds for greater control and specificity.

# Azure Monitor Insights solution

# 6.1 Application Insight Configuration

Enforcement During Deployment:

* Enforce the configuration of Application Insights for Applications, Containers, VMs, Network, SQL, and Key Vault during resource deployment.

# 6.2 Data Collection Rules (DCR) Configuration

Linux VM Teant-wide Data Sources:

* Configure Performance Counters (80% as threshold for CPU, RAM) and Linux Syslog Counters for Linux VMs tenant wide.

Windows VM Teant-wide Data Sources:

* Configure Performance Counters (80% as threshold for CPU, RAM) and Windows Event Log for Windows VMs tenant wide.

# 6.3 Data Collection Rules (DCR) Automation

Automation Scope:

* Automate the configuration of VM Insights, Container Insights, and Network Insights during resource deployment via Bicep templates.

\*(use azure policy to enable Insights for respective resources)\*

# Governance

# 7.1 Diagnostic Settings Configuration

Resource Logs Enablement:

* Enable All Metric Logs and Performance Counter Logs via Data Collection Rules (DCR) for all Azure resources.

# 7.2 Monitoring Application with Application Insight

Centralized Log Analytics Workspace:

* Configure all metrics and logs to a central Application Log Analytics Workspace in the Hub Subscription.

Application Insight Settings:

* Enable and configure Application Insights to the same Application Log Analytics Workspace.
* Use below Policy initiative to track any azure monitor agent.

# 7.3 Monitoring VM with VM Insight

Supported Virtual Machine Types:

* Monitor Azure VMs, Azure VM Scale Sets, and VDI with Azure Monitor Insights.

Mandatory Configurations:

* Deploy Azure Monitoring Agent and configure VM data collection.
* Use Azure policy to deploy azure monitor agent if it does not exist.
* Use below AV policy to track any VMs without Azure monitor agent installed and force install the agent.

A screenshot of a chat

Description automatically generated

# 7.4 Monitoring Container with Container Insight

Supported Container Environments:

* Configure Container Insights for Azure Kubernetes Services (AKS), Azure Arc-enabled Kubernetes Cluster, and VMware Tanzu (TKG).

Mandatory Configurations:

* Deploy Azure Monitor agent for Linux, Log Analytics Agent, and Data Collection Rules for all containers.
* Use below Policy initiative to track containers without diagnostics settings enabled and enforce this settings.

A screenshot of a computer

Description automatically generated

# 7.5 Monitoring Network with Network Insight

Comprehensive Network Monitoring:

* Monitor network health metrics, connectivity, and traffic metrics with Azure Monitor Network Insights.

Network Watcher Deployment:

* Deploy Azure Network Watcher for each VNET under the standard service deployment model of an Application Landing Zone.
* Below three policy will be used to create an initiative to deploy network watcher and enable network flow logs if its missed during standard service deployment.

A white background with black lines

Description automatically generated

# 7.6 Monitoring Storage Account with Storage Insight

Unified Storage Monitoring:

* Monitor storage accounts' performance, capacity, and availability metrics with Storage Insights.

Configuration Requirement:

* Configure All Metric diagnostics logs to a central Application Log Analytics Workspace for monitoring storage accounts.

# 7.7 Govern Key Vault with Key Vault Insight

Key Vault Monitoring Metrics:

* Govern Key Vault requests, performance, failures, and latency with Key Vault Insights.

Configuration Requirement:

* Configure All Metric diagnostics logs to a central Application Log Analytics Workspace for governing Key Vaults.

# Operations

# 8.1 VM Monitoring Deployment Agent

Implementation Steps:

1. Install Agent via Bicep as Part of VM Deployment (IaC):

* Utilize Bicep templates to include the Azure Monitor agent installation as part of the virtual machine deployment process.

2. Optional Enforcement by Policy and User Managed Identity:

* Implement Azure Policy to enforce the presence of the Azure Monitor agent.
* Use user-managed identity with a condition of "If not exists" to ensure the agent is installed.

A screenshot of a chat

Description automatically generated

3. Last Resort Investigation and Installation:

* If the agent is missing, investigate from the VM Insight blade.
* Manually install the agent if it is not found.

# 8.2 Storage Account Monitoring Enforcement

Implementation Steps:

1. Enforcement of Diagnostics Settings via Code During Deployment:

* Include code in deployment scripts to configure diagnostics settings for storage accounts, including metrics, transactions, and storage logs.

2. Optional Enforcement by Policy and User Managed Identity:

* Use Azure Policy to enforce the presence of diagnostics settings for storage accounts.
* Utilize user-managed identity with a condition of "If not exists" for additional enforcement.

3. Last Resort Investigation and Enablement:

* If diagnostics settings are missing, investigate from the Storage Insight blade.
* Enable diagnostics settings manually if they are not configured.

# 8.3 Key Vault Monitoring Deployment Agent

Implementation Steps:

1. Enforcement of Diagnostics Settings via Code During Deployment:

* Include code in deployment scripts to configure diagnostics settings for Key Vaults, including all metrics.

2. Optional Enforcement by Policy and User Managed Identity:

* Use Azure Policy to enforce the presence of diagnostics settings for Key Vaults.
* Utilize user-managed identity with a condition of "If not exists" for additional enforcement.

3. Last Resort Investigation and Enablement:

* If diagnostics settings are missing, investigate from the Key Vault Insight blade.
* Enable diagnostics settings manually if they are not configured.

# Azure Monitor Access Control

# 9.1 Overview

Azure Monitor Access Control involves managing permissions and access rights for Azure Monitor resources and functionalities. This ensures that only authorized users can view, manage, and take actions on monitoring data, alerts, and dashboards.

# 9.2 Built-In Monitoring Roles

Azure provides two built-in monitoring roles for managing access to Azure Monitor resources:

* Monitoring Reader: Allows users to view monitoring data and access monitoring features but does not allow them to make any changes.
* Monitoring Contributor: Allows users to manage monitoring data, create and manage alerts, and access monitoring features.

# 9.3 Assignments

* Role Assignment: Use a Security Group to manage access to Azure Monitor resources. Assign the Monitoring Contributor RBAC role to this Security Group.
* User Assignment: Add users responsible for Azure Monitoring to the Security Group, ensuring they have the necessary permissions to perform their roles.

# 9.4 Implementation Steps

1. Create Security Group:

* Create a Security Group in Azure AD specifically for Azure Monitor access.

2. Assign Monitoring Contributor Role:

* Assign the Monitoring Contributor role to the Security Group.
* This can be done through the Azure portal or using Azure PowerShell/Azure CLI.

3. Add Users to Security Group:

* Add users responsible for Azure Monitoring to the Security Group.
* Users will inherit the Monitoring Contributor role through the group membership.

4. Verify Access:

* Test the access of the Security Group members to Azure Monitor resources to ensure they have the necessary permissions.
* Make any adjustments to role assignments or group membership as needed.

Follow the principle of least privilege when assigning roles and permissions to ensure that users only have access to the resources and functionalities necessary for their roles.

# Azure Monitor Security Control

**Design Decision**

* **Log Export:** Export Azure Monitor Logs to a Storage Account.
* **Access Control:** Control access to the Storage Account using the existing Access Review process to ensure logs are secured.

# 10.1 Implementation Steps

1. **Create Storage Account:**
   * Create a Storage Account in Azure where Azure Monitor Logs will be exported.
2. **Configure Log Export:**
   * Configure Azure Monitor to export logs to the Storage Account.
   * This can be done through the Azure portal or using Azure PowerShell/Azure CLI.
3. **Access Control:**
   * Use the existing Access Review process in AV to manage access to the Storage Account.
   * Ensure that only authorized users have access to the Storage Account.
4. **Monitor and Review Access:**
   * Implement logging and auditing on the Storage Account to track access and changes.

**Considerations**

* **Data Retention:** Define and implement a data retention policy for the logs stored in the Storage Account to comply with regulatory requirements and organizational policies.
* **Encryption:** Enable encryption on the Storage Account to protect the logs at rest.
* **Regular Audits:** Conduct regular audits of access to the Storage Account to ensure compliance with security policies and practices.

# Configuration Templates for Azure Alerts: -

## Azure Monitor Baseline Alerts: -

There is industry best practice guidance around key alerts metrics and their thresholds which can be configured as a minimum baseline for the alerts. The idea is to setup the minimum set of alerts and build upon them as needed by various teams.

The AMBA (Azure Monitor baseline alerts) is divided into two main sections:

**Azure Resources:** This section provides guidance for individual Azure resources. For each service, there is a list of key alert metrics and the recommended thresholds. We need to compare these with the list of alerts listed in this document as per the design decision and come up with the total list of baseline alerts that are relevant to AV.

**Patterns / Scenarios:** This section provides guidance for common patterns / scenarios (like Azure Landing Zones), as well as policy definition and initiatives for deploying the alerts in our environment.

[Azure Landing Zones | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/)

[Alerts Details | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/Alerts-Details/) (This section contains the list of alerts that can be deployed as part of ALZ pattern)

[Policy Initiatives | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/Policy-Initiatives/) (This section details the ALZ-Monitor Azure policy initiatives leveraged for deploying the ALZ-Monitor baselines.)

**How to deploy these AMBA:-**

We can use Azure devops pipeline or CLI to deploy these alerts. Guidance around how to deploy these alerts are available under below links.

[Introduction to deploying the ALZ Pattern | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/deploy/Introduction-to-deploying-the-ALZ-Pattern/)

[Deploy with Azure Pipelines | Azure Monitor Baseline Alerts](https://azure.github.io/azure-monitor-baseline-alerts/patterns/alz/deploy/Deploy-with-Azure-Pipelines/)

## Service Health Alert Settings

Note that these must be created for each Subscription, and they cannot span multiple subscriptions:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Alert | Services | Regions | Event Types | Action Group(s) | Description |
| shar-[subscriptionname]-allresources | All services | Australia East, Australia Southeast,  Global | All | ag-infra-01 | Notifies Infrastructure Operations team of any service health issues on any resource type |
| shar-[subscriptionname]-networkresources | Application Gateway  ASGs  Azure Firewall  Bastion Hosts  Connections  DDoS  Express Routes  Firewall Policies  IP Groups  Load Balancer  Local Network Gateway  NAT Gateways  NICs  Network Manager  NSGs  NVAs  Network Watcher  Public IPs  Private Endpoints  VPN Gateways  Route Filter  Route Table  Virtual Hubs  Virtual Network Gateway  Virtual Network  VWAN | Australia East, Australia Southeast,  Global | All | ag-network-01 | Notifies the Network Operations team of any service health issues on Microsoft.Network resource types |
| shar-[subscriptionname]-securityresources | Activity Logs & Alerts  Advisor  Alerts  Alerts & Metrics  Azure Policy  Defender  Sentinel  Key Vault  Monitor  Purview | Australia East, Australia Southeast, Global | All | ag-security-01 | Notifies the Security Operations team of any service health issues on Security related resource types |
| shar-[subscriptionname]-databaseresources | Azure Cosmos DB  Azure Cosmos DB for PostgreSQL  Azure Database for MariaDB  Azure Database for MySQL  Azure Database for MySQL flexible server  Azure Database for PostgreSQL  Azure Database for PostgreSQL flexible server  SQL Database  SQL Managed Instance  SQL Server on Azure VMs  SQL Server Stretch Database  Azure Database Migration Service | Australia East, Australia Southeast, Global | All | ag-database-01 | Notifies the Database Operations team of any service health issues on Database resource types |

## Resource Health Alert Settings

Note that these must be created for each Subscription, and they cannot span multiple subscriptions:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alert | Resource Group | Resource Type | Resource | Event Status | Current Resource Status | Previous Resource Status | Reason Type | Description |
| rhar-[subscriptionname]-allresources | All  Enable “Include all future resource groups” | All | All  Enable “Include all future resources” | All | ag-infra-01 | All | All | Notifies the Infrastructure Operations team of any service health issues on Database resource types |
| rhar-[subscripname]-networkresources | All  Enable “Include all future resource groups” | Application Gateway  ASGs  Azure Firewall  Bastion Hosts  Connections  DDoS  Express Routes  Firewall Policies  IP Groups  Load Balancer  Local Network Gateway  NAT Gateways  NICs  Network Manager  NSGs  NVAs  Network Watcher  Public IPs  Private Endpoints  VPN Gateways  Route Filter  Route Table  Virtual Hubs  Virtual Network Gateway  Virtual Network  VWAN | Australia East, Australia Southeast,  Global | All | ag-network-01 | All | All | Notifies the Network Operations team of any service health issues on Network resource types |
| rhar-[subscriptionname]-securityresources | All  Enable “Include all future resource groups” | Activity Logs & Alerts  Advisor  Alerts  Alerts & Metrics  Azure Policy  Defender  Sentinel  Key Vault  Monitor  Purview | Australia East, Australia Southeast, Global | All | ag-security-01 | All | All | Notifies the Security Operations team of any resource health issues on Security related resource types |
| rhar-[subscriptionname]-databaseresources | All  Enable “Include all future resource groups” | Azure Cosmos DB  Azure Cosmos DB for PostgreSQL  Azure Database for MariaDB  Azure Database for MySQL  Azure Database for MySQL flexible server  Azure Database for PostgreSQL  Azure Database for PostgreSQL flexible server  SQL Database  SQL Managed Instance  SQL Server on Azure VMs  SQL Server Stretch Database  Azure Database Migration Service | Australia East, Australia Southeast, Global | All | ag-database-01 | All | All | Notifies the Database Operations team of any resource health issues on Database resource types |

## Microsoft Entra Alert Settings

Note that these must be created for each Subscription, and they cannot span multiple subscriptions:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Alert | Resource Group | Resource Type | Resource | Event Status | Current Resource Status | Previous Resource Status | Reason Type | Description |
| Microsoft Entra | NA | Microsoft Entra Identities and Groups | All | NA | NA | NA | All | Notifies the IDAM team of any service health issues on Entra resource types |

## Metric Alert Settings

### Azure Application Gateway

The following alerts should be configured for the Application Gateway to alert for unhealthy backends and failed responses:

|  |  |
| --- | --- |
| Alert Setting | Alert Configuration |
| **Unhealthy Host Count Alert Settings** |  |
| Signal name | Unhealthy Host Count |
| Threshold | Static |
| Operator | Greater Than |
| Unit | Count |
| Threshold value | 0 |
| Action Group(s) | ag-network-01  ag-infrastructure-01 |
| Severity | 1 – Error |
| mar-appgateway-unhealthyhost-01 | Alerts the associated action groups when the Unhealthy Host value is greater than 0 |
| **Failed Request Alert Settings** |  |
| Signal name | Failed Request |
| Threshold | Static |
| Operator | Greater Than |
| Unit | Count |
| Threshold value | 0 |
| Action Group(s) | ag-network-01  ag-infrastructure-01 |
| Severity | 2– Warning |
| mar-appgateway-unhealthyhost-01 | Alerts the associated action groups when the failed request value is greater than 0 |

### Azure Virtual Machines

The out of the box settings will be configured for Virtual Machines which include:

* CPU %
* Available memory
* Data Disk IOPS
* OS Disk IOPS
* Network In Total
* Network Out Total
* VmAvailability

|  |  |
| --- | --- |
| Alert Setting | Alert Configuration |
| **CPU % Alert 1 Settings** |  |
| Alert Rule Name | mar-vm-cpupercentage-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value greater than | 80% |
| **CPU % Alert 2 Settings** |  |
| Alert Rule Name | mar-vm-cpupercentage-02 |
| Severity | 0 – Critical |
| Threshold Type | Static |
| Value greater than | 90% |
| **Available Memory Alert Settings** |  |
| Alert Rule Name | mar-vm-availablememory-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value less than | 1 GB |
| **Data Disk IOPS Alert Settings** |  |
| Alert Rule Name | mar-vm-datadiskiops-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value consumed greater than | 90% |
| **OS Disk IOPS Alert Settings** |  |
| Alert Rule Name | mar-vm-osdiskiops-01 |
| Severity | 1 – Error |
| Threshold Type | Static |
| Value consumed greater than | 90% |
| **Network In Total Alert Settings** |  |
| Alert Rule Name | mar-vm-networkintotal-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value in greater than | Will vary depending on machine. Select a value 10% higher than average Network In values over time. |
| **Network Out Total Alert Settings** |  |
| Alert Rule Name | mar-vm-networkouttotal-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Value in greater than | Will vary depending on machine. Select a value 10% higher than average Network Out values over time. |
| **VM Availability** |  |
| Alert Rule Name | mar-vm-availability-01 |
| Severity | 0 – Critical |
| Threshold Type | Static |
| Value is less than | 1 |
| **Action Group For All Alerts** | ag-infrastucture-01 |

### Storage Accounts

|  |  |
| --- | --- |
| Threshold Type | Static |
| **Availability Alert Settings** |  |
| Alert Rule Name | mar-storageaccount-availability-01 |
| Severity | 2 – Warning |
| Threshold Type | Static |
| Aggregation Type | Average |
| Value in less than | 100% |
| **Used Capacity Alert Settings** |  |
| Alert Rule Name | mar-storageaccount-usedcapacity-01 |
| Severity | 1 – Error |
| Threshold Type | Static |
| Value in greater than | 80% of capacity(selected during deployment) |

### Log Analytics

There are several out of the box alerts available for log analytics:

* When the daily cap limit is reached
* Ingestion rate limit
* Operational issues in the workspace

In the Log Analytics workspace the daily cap has not been set so cannot be configured:

|  |  |
| --- | --- |
| Alert Setting | Alert Configuration |
| **Rate Limit Alert** |  |
| Alert Rule Name | mar-loganalytics-ratelimit-01 |
| Severity | 2 – Warning |
| **Operational Issues Alert** |  |
| Alert Rule | mar-loganalytics-operationalissues-01 |
| Severity | 2 - Warning |

# 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 |

# 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.

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

**Signed on behalf of Data 3 Australia**

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