**CORE SERVICE DESIGN:**

**Azure Monitor and Insights, Log Analytics Workspace and Alerting Combined**

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, Log Analytics Workspace and Alerting Combined Core Service Design |
| **File Name** | Ambulance Victoria – Azure Monitor and Insights, Log Analytics Workspace and Alerting Combined Core Service 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 baseline design for the Azure Monitor and Insights, Log Analytics Workspace and Alerting Combined 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, Log Analytics Workspace and Alerting Combined 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, Log Analytics Workspace and Alerting Combined.

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, Log Analytics Workspace and Alerting Combined 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, Log Analytics Workspace and Alerting Combined Reliability Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **R1** | Configure service health alert rules. | Yes | Yes | IaC | At deployment |
| **R2** | Configure resource health alert rules. | Yes | Yes | IaC | At deployment |
| **R3** | Avoid service limits for alert rules that produce large scale notifications. | Yes | No | Governance | Operational – during deployment |

### Azure Monitor and Insights, Log Analytics Workspace and Alerting Combined Cost Optimisation Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **CO1** | Keep in mind that activity log alerts, service health alerts, and resource health alerts are free of charge. | Yes | No | N/A | N/A |
| **CO2** | When using log search alerts, minimize log search alert frequency. | Yes | No | Governance | Operational |
| **CO3** | When using metric alerts, minimize the number of resources being monitored. | Yes | No | IaC for recommended services, Governance | At deployment default alerts are deployed  Operationally avoid creating too many metric alerts for extra resources |
| **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 |

### Azure Monitor and Insights, Log Analytics Workspace and Alerting Combined Operational Excellence Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Checklist Item | Applicable to AV | Built Into Template | Enforcement Option | Applicability |
| **OE1** | Use dynamic thresholds in metric alert rules where appropriate. | Yes | Yes | IaC | At deployment |
| **OE2** | Whenever possible, use one alert rule to monitor multiple resources. | Yes | Yes | IaC, Governance | At deployment  Operational – avoid creating rules for each resource |
| **OE3** | To control behaviour at scale, use alert processing rules. | Yes | No | IaC | At deployment |
| **OE4** | Use custom properties to enhance diagnostics. | No | No | N/A | N/A |
| **OE5** | Use Logic Apps to customize the notification workflow and integrate with various systems. | Yes | No | Governance | Integrations require additional project work |
| **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 |

### Azure Monitor and Insights, Log Analytics Workspace and Alerting Combined 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 |

### Critical Alerts

Critical Alerts to be notified to the Action groups using SMS

Metric Alerts are alerts that are configured for specific resource types to fire when a condition of the specific metric is met. For example, when CPU exceeds 80% usage.

Log search alerts are used to monitor resources by using Log Analytics queries to evaluate logs at a set frequency. If the search finds that a condition is met, the alert will fire. This is a more advanced form of alerting that requires specific use cases.

Activity log alerts include Service Health alerts and Resource Health Alerts. Service Health Alerts cover all customers in a region meaning the service has an issue across the entire region. Resource Health alerts are specific to only your tenancy.

Finally, Smart Detection Alerts are a function of Application Insights. After initial set up it takes 24 hours for App Insights to learn the normal performance pattern of your applications. When an anomaly is detected, it will fire an alert. No specific configuration is required for this once App Insights is deployed.

## Design Decisions and Justifications for Alerts

### Notifications

**Design Reference:** N/A

**Design Decision:** E-mails will be used for notifications.

**Design Justification:** E-mail notifications are the currently adopted practice for receiving alerts. This will continue to be used as it is a currently adopted practice and requires no change to current processes. Emails will be sent to a Mailbox not to distribution list

### Alert Types

**Design Reference:** N/A

**Design Decision:** Metric, Resource Health, and Service Health alerts will be configured.

**Design Justification:** Metric, Resource Health, and Service Health alerts are broad enough to cover all major resource type requirements, without causing alert fatigue. There are also plenty of out of the box settings that can be created which minimizes the need to do additional customisation work.

### Action Groups

**Design Reference:** N/A

**Design Decision:** Action Groups will be created for the following user groups:

* Infrastructure
* Networking
* DBA
* Security
* IDAM

**Design Justification:** To ensure that teams are appropriately notified for alerts relating to their field, action groups will be created. This will allow the network team to only receive notifications relating to networking alerts as an example.

### Resource health alerts

**Design Reference:** Table 3 – [R2](#_Alerting_Reliability_Checklist)

**Design Decision:** Resource Health alerts will be configured for all resource types.

**Design Justification:** Resource Health alerts are scoped to a subscription and must be re-created on each subscription. They will be set to include all future resource groups in case more are created. All resource types will be covered, but there will also be rules created for function-specific teams such as Networking and Database.

### Service Health Alerts

**Design Reference:** Table 3 – [R1](#_Alerting_Reliability_Checklist)

**Design Decision:** Service Health Alerts will be configured for each subscription.

**Design Justification:** Service Health Alerts cannot span more than one subscription, so they are required to be re-created each time. The alerts for Service Health will be set for all resource types. There will also be rules created for function-specific teams such as Networking and Database.

### Metric Alerts

**Design Reference:** Table 4 – [CO3](#_Alerting_Cost_Optimisation) Table 5 – [OE1](#_Alerting_Operational_Excellence)

**Design Decision:** Metric alert rules will be recommended for major resources including:

* Azure Application Gateway
* Azure Virtual Machines
* Storage Accounts
* Log Analytics Workspace

Static thresholds will be used over Dynamic Thresholds.

**Design Justification:** It is generally not recommended to configure metric alerts for every single service for every metric as this will lead to alert fatigue and will result in major alerts being missed. There are several out of the box recommended alerts for resources such as Virtual Machines that will be enabled by default. The resources mentioned above have their specific recommended metric alerts in the Configuration Templates section.

Any other resources can also have metric alerts enabled as required.

Additionally, Static thresholds will be used as they grant you greater control and allow you to specify exact metrics (e.g. 90%) instead of the inbuilt dynamic thresholds (low, medium, high).

### Log Search Alerts

**Design Reference:** N/A

**Design Decision:** Log search alerts will not be configured as a default.

**Design Justification:** Log search alerts are more advanced and require specific use cases that cannot be met by other standard alerts such as metric or resource health alerts. It is recommended to create these unless necessary as it can lead to alert fatigue alongside all other alerts being created.

Solution Diagram for LAW:-



## Design Decisions and Justifications for LAW:-

### 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.

## 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 Alerts:-

## 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 | [Select value based on storage account expected use] in GB |

### 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 LAW:-

## 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 |

# 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.

Log Analytics Workspace:-

To deploy Log Analytics Workspaces according to AV’s design decisions, we can follow these steps:

Number and Location of Log Analytics Workspaces

1. **Central Log Analytics Workspaces**: Deploy a central Log Analytics Workspace in each region in the AV ALZ Management Subscription.

**2. Separate Instance for Microsoft Sentinel**: Deploy a separate instance of Log Analytics Workspace for Microsoft Sentinel.

***Logging and Monitoring***

- **Enable Diagnostic Settings**: Enable diagnostic settings for the Log Analytics Workspace itself.

- **Send Logs from Other Resources**: Configure all other resources to send their diagnostic logs to the central Log Analytics Workspace in that region.

- **Capture AllLogs and allMetrics**: Capture AllLogs and allMetrics for the Log Analytics Workspace diagnostic setting.

***Data Retention Period***

- **Set Retention Period:** Set the retention period for logs to 90 days.

***Daily Cap Limit***

- **Set Daily Cap Limit**: Set a daily cap limit of 100GB.

Azure Alerting:-

**1 Service Health Alerts**

- Create alerts for each subscription, cannot span multiple subscriptions.

- Define alerts for different service categories (Infrastructure, Networking, Security, Database) to notify respective operations teams of any service health issues.

**2 Resource Health Alerts**

- Create alerts for each subscription, cannot span multiple subscriptions.

- Define alerts for different resource types to notify the operations teams of any resource health issues.

**3 Microsoft Entra Alerts**

- Create alerts for each subscription, cannot span multiple subscriptions.

- Define alerts to notify the IDAM team of any service health issues related to Microsoft Entra identities and groups.

**4 Metric Alert Settings**

4.1 Azure Application Gateway

- Configure alerts for unhealthy backends and failed responses.

- Set static thresholds for metrics like Unhealthy Host Count and Failed Request Count.

- Define action groups to alert the infrastructure and network teams.

4.2 Azure Virtual Machines

- Configure alerts for CPU usage, available memory, disk IOPS, network traffic, and VM availability.

- Set static thresholds for CPU percentage, available memory, disk IOPS, and network traffic metrics.

- Define action groups to alert the infrastructure team.

4.3 Storage Accounts

- Configure alerts for storage account availability and used capacity.

- Set static thresholds for availability and used capacity metrics.

- Define action groups to alert the infrastructure team.

4.4 Log Analytics

- Configure alerts for rate limits and operational issues in the Log Analytics workspace.

- Set static thresholds for rate limit and operational issue alerts.

- Define action groups to alert the operations team.

# 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 |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)